МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ

МІНІСТЕРСТВО ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ІНФОРМАТИКИ І ПРАВА НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

X Всеукраїнська науково-практична конференція

Збірник тез наукових доповідей
(Київ, 4 квітня 2019 року)

Електронне видання

Київ
2019

УДК 341.123(045)(0.034.2PDF)

Організаційний комітет конференції:

Кудінов С. С. – голова організаційного комітету конференції, ректор Національної академії Служби безпеки України, кандидат юридичних наук, доцент; ***Сафонов Ю. М.*** – співголова, заступник директора з наукової роботи Інституту модернізації змісту освіти Міністерства освіти і науки України, доктор економічних наук, професор; ***Біденко А. І.*** – співголова, державний секретар Міністра інформаційної політики України; ***Пилипчук В. Г.*** – співголова, директор Науково-дослідного інституту інформатики і права Національної академії правових наук України, доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України, заслужений діяч науки і техніки України; ***Фальченко С. Л***. – проректор з наукової роботи Національної академії Служби безпеки України, кандидат юридичних наук, доцент; ***Чорний Р. Л.*** – директор науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук, старший науковий співробітник; ***Мамченко С. М.*** – директор Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, доктор педагогічних наук, професор; ***Кравець В. М.*** – заступник директора інституту (з навчальної і наукової роботи) Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, кандидат технічних наук, старший науковий співробітник; ***Климчук О. О.*** – завідувач спеціальної кафедри Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, кандидат юридичних наук, доцент; ***Гуз А. М.*** – завідувач спеціальної кафедри Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, доктор історичних наук, професор; ***Давидова Т. О.*** – в.о. заступника директора центру – начальника організаційно-наукового відділу Науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук.

Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). [Електронне видання]. – Київ : Нац. акад. СБУ, 2019. – 384 с.

У збірнику висвітлюються актуальні проблеми забезпечення інформаційної та кібернетичної безпеки України , удосконалення вітчизняного законодавства у сфері охорони державної таємниці та службової інформації, міжнародної взаємодії у сфері забезпечення інформаційної безпеки, розглядаються питання покращання змісту вищої освіти фахівців з інформаційної безпеки держави.

Для працівників органів державної влади, науковців, викладачів, фахівців з інформаційної та кібернетичної безпеки, широкої громадськості.

Тези доповідей публікуються в авторській редакції.

Організаційний комітет залишає за собою право не поділяти думку авторів.

ВСТУПНЕ СЛОВО
ректора Національної академії Служби безпеки України кандидата юридичних наук, доцента Кудінова Сергія Сергійовича

Дозвольте привітати Вас з початком роботи X Всеукраїнської науково-практичної конференції *«Актуальні проблеми управління інформаційною безпекою держави»*, присвяченої актуальним питанням інформаційної безпеки, яка є логічним продовженням фахових дискусій щодо нових трендів регіональної та глобальної безпеки, обумовлених використанням сучасних інформаційно-комунікаційних технологій.

Проведення конференції в стінах Національної академії Служби безпеки України є свідченням високого авторитету навчального закладу, який активно співпрацює з провідними вітчизняними організаціями задля вирішення безпекових проблем особистості, суспільства та держави.

Про значущість конференції свідчить той факт, що відбувається вона за сприяння та безпосередньої участі Міністерства інформаційної політики, Науково-дослідного інституту інформатики і права Національної академії правових наук України та Інституту модернізації змісту освіти Міністерства освіти і науки України.

Науковий форум є гарною нагодою осмислити і проаналізувати тактику взаємодії у сфері інформаційної безпеки, яка впливає на формування нової системи підтримання миру і сталого розвитку суспільства, на реалізацію Стратегії національної безпеки та оборони України, на функціонування механізмів протидії інформаційним загрозам та з урахуванням сучасних реалій науково обґрунтувати і окреслити перспективи подальшого розвитку системи державного управління у цій сфері.

Такі актуальні питання, як забезпечення інформаційної безпеки України, захист інформаційного простору України, формування системи забезпечення кібернетичної безпеки України, удосконалення вітчизняного законодавства у сфері охорони державної таємниці та службової інформації, міжвідомчої взаємодії у сфері забезпечення інформаційної безпеки, удосконалення змісту вищої освіти фахівців з інформаційної безпеки держави, є пріоритетом діяльності як Національної академії так і Служби безпеки України в цілому, державних установ і відомств, органів виконавчої влади, міжнародних безпекових організацій, національних урядів, зовнішньополітичних відомств, неурядових асоціацій.

То ж раді вітати сьогодні у цій залі представників Апарату Ради національної безпеки і оборони України, Міністерства оборони України, Міністерства внутрішніх справ України, Державної служби спеціального зв'язку та захисту інформації України, Служби зовнішньої розвідки України, Національного інституту стратегічних досліджень, вищих навчальних закладів та наукових установ.

Сьогодні політика України у сфері міжнародної інформаційної безпеки вирізняється достатньо високою активністю й системністю, про що свідчать зовнішньополітичні ініціативи нашої держави. Ключове значення має офіційне визнання того очевидного факту, що інформаційні технології й засоби потенційно можуть бути використані як з метою забезпечення міжнародної стабільності й безпеки, так і з метою протилежною, спрямованою на примноження загроз і викликів.

Концепт інформаційної безпеки для України розкривається через стратегію її існування як суверенної та стабільної держави, а також через розробку та впровадження цілеспрямованої системної політики захисту національних інтересів від зовнішніх та внутрішніх інформаційних загроз. Одним із шляхів реалізації цієї стратегії є освіта. Про це свідчить затвердження стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня, який відповідно до наказу МОН України №1074 від 04 жовтня 2018 року вводиться в дію з 2018/2019 навчального року. Згідно з цим стандартом Академією та іншими навчальними закладами України здійснюється переопрацювання та оновлення освітніх програм, що є актуальною темою дискусій на нашій конференції.

З метою забезпечення сектору безпеки та оборони України кваліфікованими кадрами, з 2019 року в Академії запроваджується підготовка фахівців за новою спеціальністю 256.04 Національна безпека (забезпечення державної безпеки в інформаційній сфері).

Разом з тим, у сфері державного управління інформаційною безпекою залишається безліч дискусійних та проблемних питань, які потребують наукового вирішення.

Тому сподіваюся на цікаві та інформативні доповіді та повідомлення, які цьому сприятимуть.

Будь-яка наукова конференція є не лише можливістю апробування результатів своїх наукових напрацювань та фахового спілкування. Сподіваюся, що у вас буде нагода для нових знайомств та отримання незабутніх вражень.

Дякую за увагу!

Бажаю плідної праці, конструктивних ідей та приємного спілкування!

СУЧАСНИЙ СТАН РОЗВИТКУ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

УДК 340:007

Авдошин І.В.
доктор юридичних наук,
старший науковий співробітник,
Національна академія Служби безпеки України

«ІНФОРМАЦІЙНА КАМПАНІЯ» ЯК ІНСТРУМЕНТ ВПЛИВУ НА СВІТОВУ ПОЛІТИКУ

Значна кількість міжнародних заходів сьогодні супроводжуються спеціальними інформаційними кампаніями. Поняття «інформаційна кампанія» дозволяє відрізнити одиничні дії і спонтанні інформаційні акції від комплексних, заздалегідь запланованих і погоджених дій у сфері ділових комунікацій за певною програмою. Головною причиною проведення інформаційної кампанії є необхідність інформаційної підтримки основних цілей організаторів міжнародних заходів.

Мета інформаційної кампанії при організації міжнародних заходів може бути представлена у вигляді наступного алгоритму:

- Поступове розширення зони інформації навколо теми міжнародного заходу, надання темі чіткого змісту в інтересах організаторів цього заходу.
- Цілеспрямований вплив на формування громадської думки навколо теми міжнародного заходу.
- Цілеспрямований інформаційний вплив на партнерів з метою коригування їх позиції.
- Зміна громадської думки на користь підтримки позиції «своєї» делегації на міжнародному заході.

Отже, інформаційна кампанія при організації міжнародних заходів представляє собою – заздалегідь спланований комплекс взаємопов'язаних комунікаційних дій, спрямованих на забезпечення конкретних цілей організаторів заходу шляхом цілеспрямованого впливу на громадську думку та позиції партнерів, які беруть участь у міжнародному заході.

Не секрет, що засоби масової інформації сьогодні стали найголовнішим інструментом формування громадської думки у світовій політиці. «ЗМІ фактично контролюють всю нашу культуру, пропускаючи її через свої фільтри, виділяють окремі елементи із загальної маси культурних явищ і надають їм особливої ваги, підвищують цінність однієї ідеї, знецінюють іншу, поляризують таким чином все поле культури. Те, що не по-

трапило в канали масової комунікації, в наш час майже не впливає на розвиток суспільства».

Експерти сьогодні виділяють кілька основних етапів організації інформаційних кампаній.

На першому етапі відбувається аналіз обставин, тобто проводяться необхідні дослідження і здійснюється постановка основної задачі кампанії.

На другому етапі починається розробка програми, тобто відбір каналів масових комунікацій, вибір технік впливу, визначення публіки, планування бюджету.

На третьому етапі відбувається здійснення наміченої програми, іншими словами «розкручування» теми.

Як відзначає Г. Почепцов, «реальна подія тільки тоді істотно доступна громадськості, коли про неї широкій публіці розповіли засоби масової інформації».

У період проведення міжнародного заходу здійснюється інформаційна атака або фаза активних дій у всьому інформаційному просторі.

На четвертому етапі здійснюється інформаційне прикриття (оцінка результатів кампанії, основні висновки).

Завдання інформаційного прикриття після завершення міжнародного заходу полягає в тому, щоб приховати персональну зацікавленість його ініціаторів у досягненні поставлених цілей і створити ефект максимальної об’єктивності висвітлення подій, щоб тривалі дискусії навколо теми заходу не повернули вістрі кампанії проти самих ініціаторів («ефект бумеранга»). Для цього робиться акцент на більш нейтральних сюжетах, прибирається полеміка з інформаційних повідомлень. Іноді результати вже проведеної кампанії стають основою для «розкрутки» нових тем, що дозволяє плавно перевести громадський інтерес в нове русло.

Експерти підкреслюють, що той, хто раніше з партнерів зробить висновки, що влаштовують громадськість, виявляється у виграші, в певному сенсі він сам оголошує себе переможцем.

Однак крім цього, важливо на завершальному етапі кампанії справді підвести підсумки та з’ясувати: чи вдалося дійсно досягти поставлених цілей, які були допущені помилки і як їх можна було б виправити. Саме в цьому і полягає успіх майбутніх інформаційних кампаній.

Яскравим прикладом організації та проведення успішної інформаційної компанії є інформаційний супровід американської військової операції проти Іраку, яка розпочалася у березні 2003 року. Так, напередодні військової операції проти Іраку Міністерство оборони США провело ряд міжнародних конференцій та симпозіумів, присвячених стратегії та тактиці інформаційної війни. Стратегія базувалась на масованому пропагандист-

ському ударі із використанням усіх видів ЗМІ при одночасній блокаді будь-якої інформації, яка викривала події на місці бойових дій.

Зрештою, необхідно відзначити, що фахівці зі зв'язків з громадськістю зовсім нещодавно відмовились від прийомів «жорсткої» пропаганди, що припускає яскраво виражену агресивну тональність коментарів, «гострі» зауваження на адресу опонентів, відверті технології спотворення інформації. Всі ці грубі «геббельсівські» прийоми в умовах демократії недостатньо ефективні і саме в західній демократії, але не Росії, де їх широко використовують, особливо останнім часом в умовах коли так звана російська демократія поставила себе проти всього цивілізованого світу.

Література

1. Методика формування переговорного досьє в системі Служби безпеки України : практ. посіб. [для курсантів, слухачів НА СБ України] / І.В. Авдошин. – К. : Нац. акад.. СБУ, 2015. – 242 с.

УДК 355. 402

Баліцький В.В.
кандидат юридичних наук, доцент,
Інститут Служби зовнішньої розвідки України

АКТУАЛЬНІ ПИТАННЯ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЗАКОРДОННИХ ДИПЛОМАТИЧНИХ УСТАНОВАХ УКРАЇНИ

Нарощування щодо України розвідувально-підривної та терористичної діяльності, покладають на СЗР України та СБ України актуальні завдання забезпечення інформаційної безпеки держави, зокрема, й інформаційної безпеки в її закордонних дипломатичних установах (ЗДУ).

Сучасний етап розвитку науково-технічного прогресу, використання дипломатичними службами сучасних технічних засобів обробки та передачі інформації, новітніх інформаційних технологій сформував принципово нове середовище функціонування органів дипломатичної служби за кордоном, яке містить значні ризики й загрози для їх безпечної діяльності, і в першу чергу, для ефективного здійснення ними своєї дипломатичної місії у безпечних інформаційних умовах.

Ключовими питаннями у цьому напрямі, за висновками фахівців, є забезпечення інформаційної безпеки ЗДУ, створення в них безпечних умов роботи зі службовою й конфіденційною інформацією, оперативного обміну нею з Міністерством закордонних справ України з метою своєчасного і попереджувального інформування керівництва держави й недопу-

щення нанесення їй шкоди в політичній, економічній, військово-технічній, гуманітарній та інших сферах.

Безпечне функціонування закордонних дипломатичних установ України забезпечується Міністерством закордонних справ спільно з іншими зацікавленими державними органами України, зокрема, Службою зовнішньої розвідки України, Службою безпеки України, Державною службою спеціального зв'язку та захисту інформації України, Адміністрацією державної прикордонної служби України відповідно до визначеної їм чинним законодавством компетенції.

Нормативно-правову основу системи комплексного забезпечення безпечного функціонування закордонних дипломатичних установ становлять Закони України «Про основи національної безпеки України», «Про дипломатичну службу», «Про державну таємницю», «Про інформацію», «Про розвідувальні органи України», а також «Положення про дипломатичне представництво України за кордоном», затверджене Указом Президента України від 22 жовтня 1992 року № 166/92-рп, розроблена зовнішньою розвідкою спільно з МЗС України «Інструкція про порядок комплексного забезпечення безпеки закордонних дипломатичних установ України», затверджена спільним наказом Міністра закордонних справ України та Голови Служби безпеки України (на той час зовнішня розвідка входила до складу СБ України) від 19.08.2003 року, «Інструкція про прядок реагування системи органів дипломатичної служби на загрозу вчинення терористичного акту», затверджена наказом МЗС України від 04 червня 2010 року та погоджена з Антитерористичним центром СБ України й «Інструкція про порядок взаємодії військовослужбовців ДССЗЗІ та СЗРУ в ЗДУ» від 13.07.2016 р.

Забезпечення безпечного функціонування установ України за кордоном, безпеки їх співробітників і членів сімей та відряджених за кордон українських володільців державної таємниці покладене на Службу зовнішньої розвідки України разом з іншими розвідувальними органами держави (військова розвідка – ГУР Міністерства оборони України та розвідка Державної прикордонної служби), згідно з Законом України «Про розвідувальні органи України».

На Службу безпеки України, згідно з законами України «Про Службу безпеки України» і «Про контррозвідувальну діяльність», покладаються завдання із забезпечення збереження державної таємниці в закордонних дипломатичних установах України та громадянами України за кордоном.

Також, згідно з Законом України «Про державну таємницю», Служба безпеки України здійснює державний контроль за станом охорони державної таємниці в закордонних дипломатичних установах України. За належне дотримання режиму таємності в ЗДУ загалом відповідає керівник установи, а безпосередньо організовує цю роботу офіцер безпеки.

Державна служба спеціального зв'язку та захисту інформації України («Держспецзв'язок») згідно з Законом України «Про Державну службу спеціального зв'язку та захисту інформації України», відповідає за здійснення заходів з організації й забезпечення безпеки функціонування урядового зв'язку із закордонними дипломатичними установами України, а також упровадження комплексних систем захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах закордонних дипломатичних установ України.

Разом з цим, «Держспецзв'язок» України, як уповноважений державний орган у сфері технічного захисту інформації (ТЗІ), здійснює державний контроль за станом технічного захисту та обігу класифікованої інформації в закордонних дипломатичних установах України.

У сучасних умовах організація захисту закордонних дипломатичних установ України від агентурного й оперативно-технічного проникнення іноземних спецслужб та забезпечення безпеки обігу конфіденційної інформації в них набуває все більшої актуальності і потребує постійного системного й комплексного вирішення.

Література

1. Про розвідувальні органи України: Закон України // Відомості Верховної Ради України. – 2001. – № 19. – Ст. 94.

2. Про основи національної безпеки України: Закон України // Відомості ВР України. – 2003 (зі змінами 2014р.). – №29. – Ст. 143.

3. Про державну таємницю: Закон України // Відомості Верховної ради (ВВР). – 1994. – № 16. – Ст. 650.

4. Про інформацію: Закон України // Відомості Верховної ради (ВВР). – 1992. – № 48. – Ст. 93.

УДК 323.2:342.951:351.75

Благодарний А.М.
кандидат юридичних наук,
старший науковий співробітник,
Національна академія Служби безпеки України

УДОСКОНАЛЕННЯ ПРАВОВОЇ РЕГЛАМЕНТАЦІЇ ПРОТИДІЇ ЕКСТРЕМІЗМУ

Раніше вітчизняними науковцями екстремізм досліджувався переважно на прикладі інших країн [1], але останнім часом через неоголошену збройну агресію Російської Федерації в Україні значно активізувалася діяльність екстремістських угруповань, особливо політичного спрямування. Значна частина цих угруповань керується і оснащується російськими спецслужбами в межах таємних заходів розвідувально-підривної війни

проти України. Екстремісти використовують складне соціально-економічне становище, зумовлене воєнними діями на території Донецької та Луганської областей, для дестабілізації внутрішньої обстановки, дискредитації органів публічної влади перед міжнародними партнерами та Українським народом, провокації безладів і масових порушень громадського порядку [2].

Виходячи з викладеного, в сучасних умовах становлення громадянського суспільства одним із актуальних завдань розвитку вітчизняного права є розробка нормативної основи протидії екстремізму у різних його проявах.

Аналіз останніх досліджень і публікацій засвідчує, що у науковій царині відсутній єдиний підхід до визначення поняття екстремізму, але найчастіше цей термін розуміється як соціально-політичний феномен, що становить собою сукупність ненасильницьких і насильницьких крайніх форм не прийняття алгоритму соціального управління в певному соціумі [3].

У вітчизняній юридичній літературі простежуються два основних підходи до правової регламентації протидії екстремізму. Так, деякі науковці, ураховуючи, що екстремістська діяльність створює передумови до проведення терористичної діяльності, пропонують передбачити відповідні зміни щодо закріплення визначення екстремістської діяльності та екстремістських матеріалів у Законі України «Про боротьбу з тероризмом» [4, с. 64]. Інші фахівці пропонують опрацювати проект окремого Закону України «Про протидію екстремізму» [5]. Оскільки екстремістські прояви можуть мати ознаки як кримінального, так і адміністративного правопорушення, то прихильники обох підходів погоджуються у тому, що слід внести відповідні зміни до КК України та КУпАП. Як влучно зауважив Д. Лук'янець, інститути адміністративної і кримінальної відповідальності разом створюють, так би мовити, захисну оболонку для різних суспільних відносин. При цьому адміністративна відповідальність може розглядатись як профілактичний засіб щодо багатьох видів злочинних діянь, за які передбачена кримінальна відповідальність [5, с. 137].

Вважаємо, що у системі заходів, які вживаються органами державної влади щодо припинення, блокування та нейтралізації екстремістських проявів і забезпечення безпеки населення України, значну роль мають відігравати заходи адміністративного примусу. Застосування зазначених заходів повинно запобігати злочинним проявам екстремізму, тому пропонуємо передбачити адміністративну відповідальність за замовлення, виготовлення, зберігання та розповсюдження екстремістських матеріалів. Правові норми зазначеної спрямованості законодавчо закріплені у таких країнах як Великобританія, Республіка Чехія, Республіка Білорусь, Республіка Казахстан та багатьох інших. Як засвідчує іноземний досвід застосування заходів із протидії екстремізму, запобігти зазначеному явищу можна лише спільними зусиллями державних органів та громадськості, спрямованими на підвищенням правової і загальної культури населення, поліпшення соціально-економічних умов життя людей, формування позитивного іміджу держави.

Таким чином, удосконалення норм кримінальної та адміністративної відповідальності (зокрема, запровадження адміністративної відповідальності за замовлення, виготовлення та поширення екстремістських матеріалів) з обов'язковим детальним роз'ясненням громадськості причин запровадження вказаних заходів дозволить вітчизняним правоохоронним органам більш ефективно протидіяти екстремістським проявам, але при реформуванні зазначеного законодавства обов'язково слід врахувати досвід провідних держав світу та виходити не лише з інтересів певних міністерств та відомств, а також і врахувати громадську думку з цього питання.

Література

1. Рева Т.С. Сучасний політичний екстремізм (на прикладі Іспанії, Італії та Німеччини) : дис ... канд. політ. наук: 23.00.02 / Т.С. Рева . – Київ : Київський національний університет імені Тараса Шевченка., 2012 . – 211 с.

2. Булгаков А.О. Співробітництво України з міжнародними організаціями у сфері протидії політичному екстремізму / А.О. Булгаков // Науково-практична інтернет-конференція «Проблеми реалізації та забезпечення ефективності правових реформ» 16 червня 2016 року. URL: http://legalactivity.com.ua.A110616-11&catid. (дата звернення 22.02.2019).

3. Майоров В.В. Розмежування терористської та екстремістської діяльності. URL: http://goal-int.org/rozmezhuvannya-teroristskoi-ta-ekstremistskoi-diyalnosti. (дата звернення 22.02.2019)

4. Ірха Ю.Б. Використання екстремістами мережі Інтернет: правові проблеми виявлення та протидії в Україні / Ю.Б. Ірха // Інформація і право . – 2015. – № 3(15). – С. 56 – 65.

5. Висновок Головного науково-експертного управління Верховної Ради України на проект Закону України "Про протидію екстремізму" (реєстр. № 9156 від 15 верес. 2011 р.). URL: http://w1.c1.rada.gov.ua/pls/zweb_n/webproc4_1 pf3511. (дата звернення 22.02.2019)

6. Адміністративне право України. Академічний курс: Підруч.: У двох томах: Том 1. Загальна частина / Ред. колегія: В. Б. Авер'янов (голова). – К,: Видавництво «Юридична думка», 2004. – 584 с.

УДК 340:351.86

Богуцький П.П.
кандидат юридичних наук, доцент,
Науково-дослідний інститут
інформатики і права НАПрН України

ПРАВО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМІ ПРАВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Забезпечення інформаційної безпеки суспільства і людини полягає в організації та здійсненні відповідного комплексу заходів, серед яких важ-

ливе місце належить правовим чинникам. Примітно, що проблема правового забезпечення інформаційної безпеки знаходить вирішення у роботах науковців, які відносять вказану проблему до сфери інформаційного права (Б.А.Кормич, О.Г.Ярема, С.С.Єсімов) або ж,насамперед, до сфери національної безпеки (Довгань О.Д., Беляков К.І.,), проте практично в усіх наукових розробках особливо відзначається комплексний характер цієї проблеми.

Зрештою, наукові дискусії щодо місця права інформаційної безпеки у системі національного права мають не лише теоретичний характер. Прикладне значення успішного вирішення цієї проблеми дозволяє зосередити зусилля на підвищенні ефективності правового регулювання усіх питань, які стосуються організації та здійснення інформаційної безпеки у контексті загальносуспільних, галузевих проблем та проблем інформаційної безпеки людини. У зв'язку з цим особливо актуальним є вплив права інформаційної безпеки на управління інформаційною безпекою держави, що є вкрай важливим для сучасної інформаційної політики України.

Певні протиріччя у розумінні змісту та сутності нормативно-правового регулювання інформаційної безпеки знято з прийняттям та затвердженням Доктрини інформаційної безпеки України [1], положення якої наразі потребують вжиття більш системних заходів щодо їхньої реалізації, упровадження у практику соціальних комунікацій.

Зрештою, сама Доктрина інформаційної безпеки України дає відповідь стосовно вирішення проблеми належності правової системної спільності, якою є право інформаційної безпеки, до системи національної безпеки. Проте такий висновок не знімає жодним чином питання щодо внутрішніх зв'язків права інформаційної безпеки з інформаційним правом.

Слушними є зауваження О.Г.Яреми та С.С.Єсімова про те, що в основі формування структурного утворення в системі права, спрямованого на забезпечення правового захисту інтересів суб'єктів інформаційної сфери, є об'єктивні чинники, зокрема,відокремлення предмета правового регулювання – відносин, пов'язаних із забезпеченням захищеності найзначущих інтересів особистості, суспільства та держави в інформаційній сфері від внутрішніх і зовнішніх загроз, які є різновидом інформаційних правовідносин, що виникають у процесі діяльності щодо забезпечення інформаційної безпеки [2, с. 246]. Проте неможливо не звернути увагу на іншу важливу обставину – предмет правового регулювання є лиш одним із чинників, які дозволяють об'єктивувати правові спільності у системі права. Не будемо акцентувати увагу на дискусіях стосовно цього, але зосередимось на тому, що лінійне бачення утворення компонентів системи права не завжди дає відповідь на питання природи таких компонентів, їхнього інституційного та функціонального походження. Для наукового вирішення цієї проблеми необхідним є використання міждисциплінарного підходу, а ще більшою мірою – нелінійних характеристик як національної системи права, так і компонентів, що утворюють систему права [3, с.186-187].

Видається, що парадигма правового режиму інформаційної безпеки, яка безумовно містить предмет, метод і мету правового регулювання, дозволяє дати більш ґрунтовну відповідь на системну належність права інформаційної безпеки. Мета права інформаційної безпеки – у створенні таких правових умов, за яких стан захищеності систем обробки і зберігання даних, конфіденційність, доступність і цілісність інформації стають досяжними, тобто забезпечуються. По-іншому – інформаційна безпека і є метою права інформаційної безпеки, що суттєво впливає на визначеність цієї правової спільності у системі права. Водночас, національна безпека не уявляється без забезпечення інформаційної безпеки, а тому у більш широкому розумінні право інформаційної безпеки є складовою права національної безпеки України. Право інформаційної безпеки має складну структуру, яка містить інститути права безпеки інформаційних технологій, безпеки інформаційних систем тощо.

Можливим є виокремлення певної системної групи норм права, які регулюють суспільні відносини щодо управління інформаційною безпекою держави, та відображають їхню належність до права інформаційної безпеки. Висловлене бачення сутності та змісту права інформаційної безпеки дозволяє більш системно і послідовно здійснювати правовий вплив на соціальні комунікації у галузі інформаційної безпеки, що позитивно має позначатися на ефективності реалізації інформаційної політики держави, Доктрини інформаційної безпеки України.

Література

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року №47/2017 // База даних «Законодавство України» // ВР України. URL:https://zakon.rada.gov.ua/laws/show..... (дата звернення 6.03.2019).

2. Ярема О.Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві / О.Г.Ярема, С.С.Єсімов // Науковий вісник Львівського державного університету внутрішніх справ. – 2016. – № 2. – С. 244-252.

3. Богуцький Павло. Нелінійна раціональність системи права / Павло Богуцький // Право України. – 2018. – № 6. – С. 182-195.

УДК 35.078.3

Бондаренко І.Д.
Національна академія СБ України

ІНФОРМАЦІЙНА СКЛАДОВА ГІБРИДНОЇ ВІЙНИ РФ ПРОТИ УКРАЇНИ

В Концепції зовнішньої політики РФ 2016р. зазначено: «РФ зацікавлена у розвитку всього різноманіття політичних, економічних, культурних

і духовних зв'язків з Україною, на основі взаємоповаги. Росія докладатиме необхідних зусиль для політико-дипломатичного врегулювання внутрішнього українського конфлікту». Цинізм цієї декларативності є надяскравим, адже в реальності метою РФ є руйнація української державності шляхом використання «брудних» інструментів гібридної війни.

Як вважають міжнародні аналітики, для досягнення своїх цілей РФ може використовувати два сценарії. Перший: формування в суспільстві джерел нестабільності, конфліктів, на базі цього повна зміна державницького курсу України, формування лояльної, контрольованої РФ влади. Другий: федералізація України з можливістю регіонів впливати на зовнішню політику і політику безпеки держави, що дасть можливість загальмувати європейську інтеграцію України і відмовитися від курсу вступу до НАТО. Саме базу для останнього російська сторона змогла імплементувати в Мінських домовленостях, де головною вимогою до України є надання особливого статусу районам, контрольованим «ДНР-ЛНР».

Указ В.Путіна від 18 лютого 2017р. про визнання паспортів і інших документів ДНР-ЛНР, введення «указом» Захарченка з 27 лютого «державного кордону» ДНР з Україною, а також захоплення бойовиками ДНР-ЛНР понад півсотні українських великих промислових підприємств на територіях цих «республік» – це підштовхування Донбасу до «точки неповернення», кроки до реалізації «осетино-абхазького сценарію», апробованого Росією після війни з Грузією, коли у серпні 2008 р. Росія визнала незалежність Абхазії і Південної Осетії, а в вересні підписала з ними договори «Про дружбу, співробітництво і взаємну допомогу».

Для здійснення деструктивного для національної державності впливу на українське населення РФ використовує повний спектр російських медіа-ресурсів, окремі пропагандистські джерела радикальної спрямованості на території ЄС, ресурси так-званих ЛНР-ДНР, які контролюються російськими спецслужбами. В останніх сформовано: 7 телеканалів (Перший республіканський, «Юніон», «Оплот», «Новороссія» тощо), 4 радіостанції і 13 республіканських газет. Всі вони прямо керуються Міністерством пропаганди. В «республіках» написана своя окрема історія, культ терористичних лідерів пропагується в школах на «уроках громадськості». Заборонені українські організації, партії, зокрема парламентські партії «Свобода», «Радикальна партія», «Народний фронт».

Початковим етапом інформаційної складової гібридної війни РФ проти України можна вважати 2007-2008 рр., коли РФ активно закріплювала в українському інформаційному просторі теми і меседжі, що мали підготувати цільову аудиторію до подальшої збройної агресії, стимулювати перехід на сторону супротивника під час активної фази протиборства. Активна фаза інформаційної війни розпочалась восени 2013 року напередодні Ві-

льнюського саміту, де планувалося підписання Угоди про асоціацію Україна-ЄС. Наразі РФ просуває такі основні пропагандистські меседжи:

- за допомогою Заходу відбувся антиконституційний заколот і до влади прийшли «бандерівці», які розв'язали геноцид проти російськомовного населення і братовбивчу громадянську війну;
- русофобська київська влада проводить каральну операцію проти повстанців Донбасу;
- вороги Росії втягують Україну до ЄС і НАТО всупереч волі її народу;
- Україна – «держава, яка не відбулася» і без Росії її чекає деградація і розпад.

Слід зазначити, що до недавня Україна була абсолютно незахищеною від російської медіа-агресії. Зокрема: а) Росія мала абсолютну перевагу в інформаційному просторі України і в системі електронних та друкованих ЗМІ і в книжковому видавництві; б) критичним фактором була наявність «п'ятої колони» в системі українських ЗМІ, в органах влади, громадських об'єднаннях і політичних партіях; в) в інформаційній експансії РФ активно використовувала проросійські настрої значної частини населення східних регіонів України; г) сприятливими умовами для медіа-агресії є відсутність мовних бар'єрів, ментальна схожість громадян обох країн, спільне історичне минуле, певна близькість національних культур, величезна система родинних контактів тощо.

На противагу російській інформаційній агресії в Україні схвалено Доктрину інформаційної безпеки, створено Міністерство інформаційної політики, почала діяти Мультимедійна платформа іномовлення України, у 2015-2016 рр. українська сторона ввела пакетні санкції проти російських ЗМІ, журналістів, діячів культури, видавництв тощо, український Уряд зупинив дію міжурядової угоди з РФ про співробітництво у сфері телебачення і радіомовлення, протягом 2014-2016 рр. Національна рада з телерадіомовлення заборонила ретрансляцію 78 російських телеканалів, Державне агентство України з питань кіно відмовило у прокаті і трансляції понад 500 російських фільмів і серіалів.

Але слід констатувати, що наразі політика протистояння російській медіа-експансії переважно зводиться до максимальної мінімізації російської присутності в національному інформаційному просторі. Однак, загалом контрзаходи української сторони є часто ситуативними, не повною мірою відповідають масштабам російської експансії. Тому однією із ключових задач на фронті контрпропаганди в середній перспективі має бути створення якісного конкурентоспроможного національного інформаційного продукту. Та його популяризація серед населення.

УДК 343.341:323.28
Варенья Н.М.
кандидат юридичних наук,
Національна академія Служби безпеки України

КОНЦЕПТУАЛЬНІ ЗАСАДИ ЕФЕКТИВНОГО ІНФОРМАЦІЙНОГО ПРОТИСТОЯННЯ В УМОВАХ КОНСЦІЄНТАЛЬНОЇ ВІЙНИ

Інформаційна війна набуває рис системного протиборства, а інфосфера стає середовищем, у якому цілком можливою є реалізація загроз безпеці та стабільності країн, що змушує змінювати підходи до інформаційного протиборства та організації оперативної діяльності [1]. Питання антитерористичної безпеки і розробки пошукових запитів за контентом щодо виявлення ризиків та загроз терористичного характеру постало предметом активного наукового пошуку.

Засоби масової інформації можна вважати одним із головних інститутів сучасного суспільства, які, акумулюючи, аналізуючи та видаючи інформацію в зручному для сприйняття вигляді (або вигідному), відіграють величезну роль у формуванні масової суспільної свідомості, впливає на політику та розвиток громадської думки в цілому.

Специфічною формою сучасного тероризму є консцієнтальна війна (лат. *conscientia* – свідомість, сумління) – війна на ураження свідомості, руйнування ідентичності, а також самої здатності людини до самоідентифікації. До особливостей консцієнтальної війни відносять такі риси, як: латентність упродовж тривалого часу; різноманітність, гнучкість та непередбачуваність засобів впливу; застосування насильницьких методів викривлення інформаційно-комунікативного простору; стирання чіткого розмежування «друг-ворог»; руйнування духовних цінностей, уявлень про добро і зло, здатності людини до вільної самоідентифікації та інші. Одним із найсильніших засобів інформаційного впливу розробники концепції консцієнтальної війни вважають використання екранних технологій (поширення брехні, підкріпленої теле- або інтернет-картинками) [2].

В умовах консцієнтальної війни у відповідь необхідно використовувати цілий комплекс заходів – від моніторингу до широкого інформаційно-пропагандистського впливу на аудиторію. Важливо також враховувати емоційний стан соціальної групи, на яку здійснюватиметься компенсаційний інформаційний вплив, інакше результати можуть завдати більше шкоди, ніж бездіяльність. Тому моніторинг повинен охоплювати не лише події в реальному та інформаційному просторах, а й фіксувати загальний емоційно-психологічний фон і динаміку його змін.

Системний підхід до вирішення питань інформаційної безпеки дає змогу закласти комплекс заходів щодо парирування загроз інформаційній безпеці вже на стадії проектування, позбавивши себе від зайвих витрат надалі. Встановлення та осмислення принципів антитерористичної діяльності в інформаційному просторі має спиратися на всебічний аналіз суті, норм та методів сучасного тероризму. Це дасть можливість розробити комплекс відповідних та дієвих заходів із нейтралізації медіа-тероризму [3].

Об'єм інформації, швидкість, мультимедійність, анонімність, низькі витрати та глобальність дали можливість терористам подолати так зване «управління сприйняттям» («perception management»). Терористи можуть зобразити себе точно такими, якими хочуть здаватися, а також уникнути фільтрів, що накладаються традиційними ЗМІ [4].

Умовно можна визначити основні напрями впливу терористичного характеру, що здійснюється із використанням ЗМІ:

1. Психологічний та ідеологічний вплив на свідомість мас. Широко використовується у психологічній війні терору й антитерористичних заходів.

2. Пошук ресурсів, засобів, інвестицій, резервів та прихильників.

3. Збирання і розміщення інформації, що здійснюється через пошук та аналіз мап, схем, планів, місць особливо небезпечних об'єктів, отруйних та інших речовин, боєприпасів тощо.

4. Координація дій та планування терактів. Використання досягнень інформаційних технологій для спрощення, здешевлення та ефективності завуальованої координації шляхів, використання відео- та аудіоможливостей засобів масової комунікації.

Із метою оптимізації заходів щодо реалізації державної політики у сфері інформаційної безпеки, на нашу думку, необхідні подальші дії на таких стратегічних напрямах:

- оперативність прийняття управлінських рішень з урахуванням матриць наслідків та загроз, складених за результатами моніторингу;

- корекція інформаційних заходів з урахуванням реакції аудиторії.

Застосування цих напрямів дозволить значно підвищити рівень заходів, спрямованих на зменшення напруженості в суспільстві, та збільшити ступінь довіри населення до представників влади, а також у подальшому оперативно забезпечувати безпеку в інформаційному просторі. Це дасть змогу здійснювати обіг інформації із подвійним зворотним зв'язком (у т.ч. через аналіз медіа-контенту в ЗМІ та засобах масової комунікації), що дозволить максимально швидко відстежувати оперативний стан на місцях.

Література

1. Облачные вычисления стратегический ресурс ведения сетецентрических войн [Текст] / В. Р. Григорьев, А. А. Новиков // Вестник РГГУ. 2013. № 14 Серия «Информатика, защита информации, математика». С. 75-100.

2. Панарин И. Н. Технология информационной войны. М.: «КСП+», 2003. 320 с.
3. Варенья Н. М. Щодо методів виявлення небезпек та загроз терористичного характеру // Верховенство права у процесі державотворення та захисту прав людини в Україні: тези міжнародної наук.-практ. конф. (Одеса, 12-13 лютого 2016 року). Одеса: ГО «Причорноморська фундація права», 2016. С. 104-108.
4. Hoffman B. Inside Terrorism. N.Y.: Columbia University Press, 2006. P. 202.

УДК 351.746:007

Варенья Н.М.
кандидат юридичних наук,
Національна академія Служби безпеки України,
Авраменко С.І.
офіцер запасу Служби безпеки України

ІДЕОЛОГІЧНЕ ПІДҐРУНТЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ЯК ФОРМА ПРОТИДІЇ ІНФОРМАЦІЙНІЙ АГРЕСІЇ

Більшість проблем розвитку медіа-сфери України наразі викликані інформаційною війною у медіапросторі. У якості протидії інформаційній агресії рішення органів влади, перш за все, були і продовжують бути зведені до обмеження доступу до небезпечного або небажаного контенту. Проте, такі дії не можуть являти собою довгострокову стратегію. Необхідна системна робота з населенням з метою виховання підготовленого споживача інформаційного контенту.

Найбільш складним, проте достатньо ефективним методом протидії інформаційній війні є підвищення аналітичних здібностей суспільства, навчання методам критичного аналізу повідомлень, убезпечення від інформаційних диверсій [1].

На думку експертів, для України застосування контрпропаганди не є доцільним, оскільки реактивна позиція є помилковою: бути завжди позаду, когось наздоганяти, викривати фейки замість творення власного наративу та власної історії [2]. Українське суспільство перебуває між двома формами тиску на масову свідомість. З одного боку, багатьма політичними силами експлуатуються рецидиви тоталітарної спадщини. З другого – новітні технології уможливлюють набагато більш ефективніші форми ідеологічних впливів [3, с. 30]. Ідеологія (від гр. idea – поняття + logos – слово) нерозривно пов’язана з політикою і грає виключно важливу роль в політичному житті суспільства. Вона сформувалася як інструмент вираження і захисту інтересів різних соціальних груп і класів. Основне призначення ідеології – висловлювати в узагальненій формі ідейно-ціннісні основи суспільного устрою, давати відповідні орієнтири соціально-політичній по-

ведінці та діям. Одна з важливих завдань ідеологічної боротьби – впровадити в свідомість людей ідею спільності інтересів всіх класів і соціальних груп даного суспільства. У такому разі протидія у інформаційних протистояннях не потребуватиме значних зусиль з розвінчування фейків та пропагандистських кліше, тим більше, що аудиторії, які сприймають ці фейкові або перекручені інформаційні посили, та такі, що відвідують інформаційні ресурси, присвячені спростуванню цих посилів, практично не перетинаються в інформаційному просторі.

Задовольнити вимоги, що їх висувають експерти та громадяни до інформаційної протидії держави, з урахуванням ідеологічної складової, є можливим через застосування стратегічних комунікацій. У найбільш широкому розумінні стратегічні комунікації є процесом інтеграції досліджень сприйняття аудиторії та зацікавлених сторін (стейкхолдерів) і врахування отриманих результатів під час планування й реалізації політики та вжиття окремих заходів. Стратегічні комунікації по суті означають обмін (тобто під час спілкування) смислами / ідеями на підтримку національних цілей (тобто стратегічно) [4].

Термін «стратегічні комунікації» вперше було введене Вінце Вітто (Vince Vitto) – головою Цільової групи з поширення керованої інформації Ради з оборонної науки, Пентагон, США у 2001 році [5]. У військово-політичному лексиконі Європи він почав використовуватися у 2006 р. Відтоді «стратегічні комунікації» як поняття й відповідна діяльність стали складником доктрини, структур і операцій НАТО. Стверджується, що США і НАТО свідомо обрали це досить розпливчасте поняття через його нейтральність і місткість, адже такі поняття, як «інформаційний вплив» і «психологічні операції» надмірно асоціюються з маніпулюванням, дезінформацією та експлуатацією [6].

Стратегічні комунікації застосовують у спосіб набуття визнання й підтримки з боку місцевого населення, електорату своєї країни, міжнародної спільноти та усіх інших цільових груп та можуть спрямовуватися на делегітимізацію та виклику в аудиторії почуттів зневіри до противника. Сутність стратегічних комунікацій полягає в тому, що сформульовані для різних цільових аудиторій меседжі не конфліктують (не протирічать) один з одним. Ефективними вважаються такі стратегічні комунікації, що не вичерпуються спрямуванням на одну конкретну цільову аудиторію, а беруть до уваги ймовірні наслідки сприйняття конкретного меседжу всіма іншими можливими цільовими аудиторіями. Відтак, змістовим ядром стратегічних комунікацій є формування стратегічного наративу – переконливої сюжетної лінії, яка може пояснити події аргументовано і з якої можна дійти висновків щодо причин знаходження держави в конфлікті, значення цього становища та щодо перспектив держави у разі успішного виходу з

нього. Такий наратив формується на підставі існуючих у суспільстві уявлень і цінностей. Стратегічні наративи навмисно побудовані або посилені з ідей і думок, які вже циркулюють, вони пропонують інтерпретацію ситуації та підказують відповіді [7].

Таким чином, варто зазначити, що наступними кроками у протидії інформаційній агресії повинні бути не лише спростування фейків та перекручувань. Головний акцент необхідно робити на якісну ідеологічну складову та використання стратегічних комунікацій для створення відповідних наративів, які б відповідали цінностям і інтересам цільових аудиторій та пропонували шляхи і способи досягнення мети, забезпечуючи соціум розумінням подій.

Література

1. Нерсесян Г.А. Медіаграмотність молоді – запорука протидії інформаційній агресії. Інвестиції: практика та досвід. – № 6. – 2018. – С. 56-60.

2. Протидія російській інформаційній агресії: спільні зусилля задля захисту демократії. Матеріали круглого столу/ URL: http://osvita.mediasapiens.ua/monitoring/advocacy_and_influence/ vlasniy_narativ_zamist_kontrpropagandi/.

3. Квіт С. М. Масові комунікації. Підручник. К.: ВД "Києво-Могилянська академія". 2008. – 206 с.

4. Department of Defense: Report on Strategic Communication. URL: http://www.au.af.mil/au/awc/awcgate/dod/dod_report_strategic_communication_11feb10.pdf.

5. NATO Strategic Communication: More to be Done? / Steve Tatham, Rita Le Page; National Defence Academy of Latvia Center for Security and Strategic Research. – Rīga, 2014. URL: http://www.academia.edu/6808986/NATO_Strategic_ Communication_More_to_be_done.

6. Dimitriu G. R. Winning the story war: Strategic communication and the conflict in Afghanistan / G. R. Dimitriu // Public Relations Review. Vol. 38. Issue 2. 2012. P. 195–207.

7. Freedman L. The Transformation of Strategic Affairs. Lawrence Freedman . The Adelphi Papers. London: Routledge, 2006. Vol. 45; Iss. 379.

УДК 621.396 (043.02)
Гнатюк С.О.
доктор технічних наук, доцент,
Національний авіаційний університет
Сидоренко В.М.
кандидат технічних наук,
Національний авіаційний університет
Поліщук Ю.Я.
аспірант PhD,
Національний авіаційний університет
Тараненко К.О.
студент,
Національний авіаційний університет

ОЦІНЮВАННЯ МАНІПУЛЯТИВНОГО ВПЛИВУ МАСМЕДІА НА СУСПІЛЬНУ ДУМКУ

У реаліях сучасності, поняття маніпулювання масовою свідомістю є важливим питанням не лише на рівні мас медіа, але і в колах науковців. На сьогодні представлена велика кількість робіт у напрямку дослідження маніпулятивного впливу мас медіа на суспільну думку. Дослідженнями моделей впливу займалися Шиян А., Хатян А., Пелещишин А., Гумінський Р. [1]. Проте, не існує методу оцінювання маніпулятивного впливу саме мас медіа як каналу впливу, адже усі методи розглядають маніпуляції без врахування широкого спектру моделей і засобів, що використовують сучасні мас медіа [2]. З огляду на це, метою є розробка методу оцінювання маніпулятивного впливу мас медіа на суспільну думку.

Запропонований метод оцінювання маніпулятивного впливу мас медіа на суспільну думку реалізується у 8 етапів (Рис.1): 1) Оцінювання фінансових витрат; 2) Ранжування причин за ступенем їх небезпеки; 3) Визначення цілей проведення кампанії маніпулювання (КМп); 4) Визначення задач проведення КМп; 5) Визначення стратегій реалізації КМп; 6) Вибір засобів мас медіа для маніпулювання; 7) Вибір методу маніпулювання; 8) Оцінювання маніпулятивного впливу. Вхідними даними методу є такі множини: причин проведення КМп; місць дислокації; цілей проведення КМп; фокус-груп; критеріїв для оцінювання параметрів; стратегій проведення КМп; мас медіа; методів маніпуляції; «вага за критеріями». Вихідні параметри: список обраних причин, цілей, критеріїв, завдань, стратегій, методів, засобів мас медіа; значення величини та ефективності маніпулятивного впливу. Реалізація цього методу дозволяє оцінити величину маніпулятивного впливу мас медіа на суспільну думку.

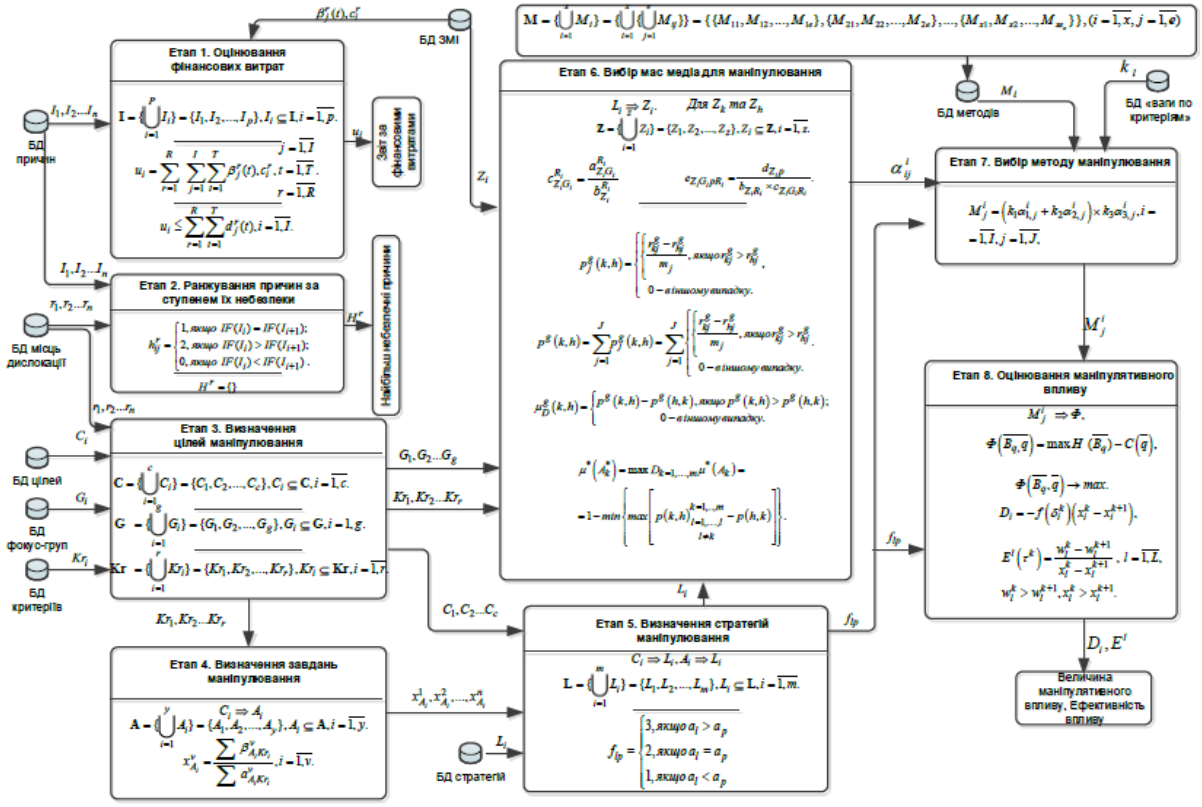


Рис. 1. Схема відображення етапів розробленого методу оцінювання маніпулятивного впливу

Етап 1 – Оцінювання фінансових витрат на КМп. У результаті виконання етапу 1 отримаємо звіт за фінансовими витратами, який необхідний для замовника. Звід допоможе зробити висновок про необхідність проведення КМп з фінансової точки зору.

Етап 2 – Ранжування причин за ступенем їх небезпеки.

У результаті виконання етапу 2 отримаємо матрицю причин, з огляду на які доцільно (чи недоцільно) проводити КМп.

Етап 3 – Визначення цілей проведення КМп. У результаті виконання етапу 3 формуються цілі, визначаються фокус-групи, на які буде націлений маніпулятивний вплив та обираються критерії за якими обираються цілі та завдання КМп.

Етап 4 – Визначення задач проведення КМп. У результаті виконання етапу 4 формуються задачі, які необхідно досягти при КМп.

Етап 5 – Вибір стратегій реалізації КМп. У результаті виконання Етапу 5 буде сформовано ряд стратегій (можливо, більше ніж 1) за якими буде реалізовуватись КМп.

Етап 6 – Вибір засобів мас медіа для маніпулювання. У результаті виконання етапу 6 буде відібрано засіб мас медіа, що за критеріями має найвищу оцінку. Не обов'язково це буде один засіб мас медіа для всіх місць дислокації, допустимо вибирати різні мас медіа для різних місць дислокації.

Етап 7 – Вибір методу маніпулювання. У результаті виконання етапу 7 вибираються методи маніпулятивного впливу, які будуть реалізовуватись тими засобами мас медіа, що вибрані на етапі 6.

Етап 8 – Оцінювання маніпулятивного впливу. У результаті отримаємо кількісний показник ефективності маніпулятивного впливу мас медіа.

На основі розробленого методу було проведено експериментальне дослідження маніпулятивного впливу вітчизняних мас медіа на суспільну думку, що дозволило провести верифікацію методу, а також встановити можливість практичного застосування для підвищення інформаційно-психологічної безпеки громадян, суспільства та держави. Отже, розроблено метод оцінювання маніпулятивного впливу, який за рахунок оцінювання фінансових витрат, визначення цілей, завдань і стратегій маніпулювання, вибору мас медіа та класифікованих методів маніпулювання, на ос-нові сформованих баз даних причин, цілей критеріїв, фокус-груп та мас медіа, дозволяє обчислювати кількісні параметри, що характеризують величину маніпулятивного впливу мас медіа на суспільну думку. Цей підхід, на відміну від відомих, дає можливість оцінити маніпулятивний вплив, що реалізується через сучасні мас медіа і використовує методи маніпулятивного впливу на суспільну думку. Отримані результати можуть використовуватися у галузі інформаційної безпеки держави, зокрема для оцінювання маніпулятивного впливу мас медіа на суспільну думку чи на свідомість окремих громадян.

Література

1. Yu. Polishchuk, S. Gnatyuk, N. Seilova. «Mass media as a channel of manipulative influence on society», Ukrainian Scientific Journal of Information Security. Vol. 21, issue 3. 2015. P. 301-308.

2. Yu. Polishchuk, T. Zhmurko. «Information-psychological security of society in the context of information warfare»: monograph. Akademia Techniczno-Humanistyczna, Bielsko-Biała, 2016. P. 321-341.

УДК 303.725.22:351.864.1 => 65.012.8(477)=161.2

Гордієнко С.Г.
доктор юридичних наук, доцент,
Національний технічний університет України
«Київський політехнічний інститут ім. Ігоря Сікорського»

СУЧАСНІ ДОКТРИНАЛЬНІ ПОЛОЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Як нами вже неодноразово зазначалося, законотворець і законодавець України має надто слабке уявлення про суть та механізми законотворення. У них також повністю відсутнє розуміння різниці між такими поняттями та категоріями, як доктрина, концепція, стратегія, програма, тактика тощо. Здається, також, що останнім невідомий причинно-наслідковий зв’язок між соціально-політичними явищами і в першу чергу кодексами, законами, постановами Верховної Ради України, нормативно-правовими актами

Президента та Кабінету Міністрів України, які у парламентсько-президентській республіці мають своє чітко визначене значення, а відповідно і "вагу".

Виходячи з визначень, що доктрина — це керівний теоретичний чи політичний принцип; концепція — система поглядів на явища, єдиний, визначальний задум; стратегія — загальний, недеталізований план певної діяльності, який охоплює тривалий період; програма — заздалегідь затверджена (визначена) дія; тактика — концептуальна дія, яка здійснюється у вигляді одного або більшої кількості конкретних завдань, стає очевидним те, що: доктрина має прийматися таким правовим актом, як Закон України на строк до 20 років), концепція - Постановою Верховної Ради на строк до 10 років, стратегія - Указом Президента України, і як свідчить світова практика - на час його обрання, програма - центральними органами виконавчої влади на 1 рік з визначеними тактичними методами її виконання.

Але як було зазначено вище, наш нормотворець йде своїм, відомим тільки йому шляхом, всупереч здоровому глузду.

В сучасних умовах розвитку української державності, спочатку приймаються: Постанова Кабінету Міністрів, далі - Укази Президента стосовно питань інформаційної безпеки і лише потім Закон України глобального для держави значення "Про національну безпеку України", яким не передбачено внесення змін до нормативних актів Президента та Кабінету Міністрів України стосовно питань інформаційної безпеки.

Далі вважаємо за доцільне їх коротко прокоментувати.

1. Постанова Кабінету Міністрів України від 14 січня 2015 р. № 2 "Питання діяльності Міністерства інформаційної політики України", якою затверджено "Положення про Міністерство інформаційної політики України" носить суто політичний характер задля протидії інформаційній пропаганді Російської Федерації в умовах громадянського конфлікту на території України і не враховує все різноманіття інформаційної політики України:

- ... Міністерство інформаційної політики України (МІП) є головним органом у системі центральних органів виконавчої влади у сфері забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів…

- Основними завданнями МІП є:

1) забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів;

2) забезпечення здійснення реформ засобів масової інформації щодо поширення суспільно важливої інформації.

- МІП відповідно до покладених на нього завдань:

- узагальнює практику застосування законодавства з питань, що належать до його компетенції, готує пропозиції щодо вдосконалення законодавчих актів, актів Президента України, Кабінету Міністрів України та вносить їх в установленому порядку на розгляд Кабінету Міністрів України;
- бере участь у формуванні державної інформаційної політики;
- організовує розроблення та впровадження навчальних курсів з інформаційної політики і розробляє навчально-методичне забезпечення для навчальних закладів усіх рівнів акредитації;
- бере участь у підготовці центральними органами виконавчої влади планів і програм навчання фахівців у сфері інформаційної політики, їх професійній підготовці, перепідготовці та підвищенні кваліфікації;

МІП з метою організації своєї діяльності забезпечує в межах повноважень, передбачених законом, реалізацію державної політики стосовно державної таємниці, захист інформації з обмеженим доступом, а також технічний захист інформації, контроль за її збереженням в апараті МІП.

Виходячи з викладеного Міністерство інформаційної політики призначене для проведення суто пропагандистських та контрпропагандистських заходів. У такому разі, доцільно змінити йому назву, адже інформаційна політика не є за суттю лише пропагандистською.

2. Указ Президента України від 26 травня 2015 року № 287/2015 "Про стратегію національної безпеки України" є вторинним по відношенню до Закону і відповідно до Закону до нього мають бути внесені зміни, чого на жаль не сталося.

Його основними положеннями є те, що Стратегія національної безпеки України спрямована на реалізацію до 2020 року визначених нею пріоритетів державної політики національної безпеки, а також реформ, передбачених Угодою про асоціацію між Україною та ЄС, ратифікованою Законом України від 16 вересня 2014 року № 1678-VII, і Стратегією сталого розвитку "Україна - 2020", схваленою Указом Президента України від 12 січня 2015 року № 5, *але не положень Закону України!!!*

Адже визначені цілі Стратегії національної безпеки України й шляхи їх реалізації ніяким чином не відображаються структурою доктрини інформаційної безпеки держави.

Серед актуальних загроз національній безпеці України ледь прослідковуються загрози інформаційній безпеці, як-то: інформаційно-психологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу.

Далі за текстом, досить еклектично згадуються загрози в першу чергу - кібербезпеці і лише потім - безпеці інформаційних ресурсів: уразливість об’єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної та-

ємниці та інших видів інформації з обмеженим доступом тощо. Вважаємо, що все має бути якраз навпаки.

Серед пріоритетів Стратегії із забезпечення інформаційної безпеки лише один пункт відповідає базовим теоретичним положенням вчення про інформаційну безпеку: розробка і реалізація скоординованої інформаційної політики органів державної влади, тоді як інші шість є гаслами.

3. Указ Президента України від 25 лютого 2017 року № 47/2017 "Про Доктрину інформаційної безпеки України" адекватно обставинам розвитку державності зазначає, що комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації. От тільки він не визначає механізму формування системи.

Указом чітко також визначається, що правовою основою Доктрини є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287 "Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України", а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Таким чином, Указ, взагалі, не визначає конкретні закони, хоча Закон України "Про основи національної безпеки України" все ще діяв.

На даний момент чинним є закон конституційного характеру з питань інформаційної безпеки - "Про національну безпеку України" від 21 червня 2018 року № 2469-VIII, однак його положення й до цього часу не враховані в Указі "Про Стратегію національної безпеки України".

Новелою Указу є визначення стратегічних, урядових та кризових комунікацій і поняття стратегічного наративу. Але, як нами вважається, в першу чергу доцільним було б визначити поняття інформаційної безпеки України, яка є предметом регулювання даного Указу.

Метою Доктрини встановлюється уточнення засад формування та реалізації державної інформаційної політики (цікавим є питання де вони викладені - С.Г.), насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни.

Доктриною визначаються національні інтереси України в інформаційній сфері та загрози національним інтересам та національній безпеці України в інформаційній сфері, які класифіковані абсолютно еклектично:

1) забезпечення інформаційної безпеки;

2) забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію;

3) відкритості та прозорості держави перед громадянами;

4) формування позитивного міжнародного іміджу України.

Таким же чином, на превеликий жаль, викладена і структура пріоритетів державної політики в інформаційній сфері.

Вперше в указах такого характеру зустрічаємо підрозділ "Механізм реалізації Доктрини".

Його структура та зміст викликає величезні запитання до законотворця, адже абсолютно незрозуміло, яким чином задекларовані завдання міністерств, Державного агентства України, Національної ради, Державного комітету, Служби безпеки України, Розвідувальних органів України мають сприяти реалізації та захисту національних інтересів України. Не описано механізм забезпечення в межах своїх компетенцій формування і реалізації державної політики у сфері реалізації державної політики у сфері інформаційної безпеки України Державною службою спеціального зв'язку та захисту інформації України та Національним інститутом стратегічних досліджень.

Все це також дуже схоже на гасла, а не на державну політику у галузі забезпечення інформаційної безпеки України.

4. Закон України "Про національну безпеку України" від 21 червня 2018 року визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз.

Цим Законом ... запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони.

На жаль, поняття "Стратегія інформаційної безпеки" Законом не визначається, хоча інші стратегії: національної, воєнної, кібербезпеки, громадської безпеки та цивільного захисту, розвитку оборонно-промислового комплексу, як - документи довгострокового планування хоч якось змістовно визначені.

При цьому у розділі "Державна політика у сферах національної безпеки і оборони" відзначено що вона спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо.

Також у Законі зазначається, що загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки і оборони визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки і оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України.

Очевидним є доцільність визначення назв "інших документів".

Розділом IV "Сектор безпеки і оборони", визначено, що Президент України, видає укази і розпорядження з питань національної безпеки і оборони, які є обов'язковими до виконання на території України, зокрема указами Президента України затверджуються Стратегія національної без-

пеки України, Стратегія воєнної безпеки України, інші стратегії, доктрини, концепції, якими визначаються актуальні загрози національній безпеці, основні напрями і завдання державної політики у сферах національної безпеки і оборони, розвитку сектору безпеки і оборони.

Тобто, на законодавчому рівні визначається ієрархія стратегічних документів: (1) стратегії, (2) доктрини, (3) концепції, що не відповідає теоретичним положенням, викладеним вище.

Окремо визначається, що Служба безпеки України здійснює контррозвідувальний захист ... економічної та інформаційної безпеки держави.

Законом визначено, що планування у сферах національної безпеки і оборони поділяється на довгострокове (понад п’ять років), середньострокове (до п’яти років) та короткострокове (до трьох років).

Документами довгострокового планування визначені: Стратегія національної безпеки України, Стратегія воєнної безпеки України, Стратегія громадської безпеки та цивільного захисту України, Стратегія розвитку оборонно-промислового комплексу України, Стратегія кібербезпеки України та Національна розвідувальна програма.

При цьому, стратегія інформаційної безпеки не визначається самостійною.

Стратегією визначено, що вона є основою для підготовки всіх інших документів щодо планування у сферах національної безпеки і оборони.

Законом передбачено, що Міністерства та інші центральні органи виконавчої влади розробляють державні цільові програми та інші програми на основі галузевих стратегій реалізації державної політики у сферах національної безпеки і оборони у встановленому законом порядку.

Однак, як ми зазначали раніше, Міністерство інформаційної політики до свого завдання віднеслось неадекватно.

Закон не передбачає змін до стратегії інформаційної безпеки України, відповідно як і до доручень Кабінету Міністрів України стосовно приведення своїх нормативно-правових актів у відповідність із цим Законом. Останнє відноситься до компетенції Міністерства інформаційної політики, яке має продукувати, як інформаційну політику держави, так і її політику в галузі інформаційної безпеки.

Тобто застосування положення "забезпечити приведення у відповідність із цим Законом нормативно-правових актів міністерств та інших центральних органів виконавчої влади" не передбачено наведеними нормами права.

Таким чином, викладене вище слугує підставою для вкрай простого, але важливого висновку: в Україні навіть у першому наближенні відсутні ознаки політики інформаційної безпеки України, хоча теоретико-прикладних та науково-обґрунтованих теорій забезпечення інформаційної безпеки України існує чимало. Тобто влада на свій розсуд приймає правові положення без їх теоретичного обґрунтування, що і призводить до появи зазначених міністерств та нормативно-правових актів, які еклектично "регулюють" питання інформаційної безпеки України.

УДК 351
Горовий В.М.
доктор історичних наук, професор,
засл. діяч науки і техніки України
Національна академія Служби безпеки України

ГРОМАДЯНСЬКЕ ІНФОТВОРЕННЯ В ПІДВИЩЕННІ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ УКРАЇНИ

Глобальне входження цивілізації в інформаційний етап її розвитку у соціальному вимірі проявляється у вдосконаленні структури націй і держав. У цьому процесі все більшу роль будуть відігравати інформаційні параметри розвитку. У зв'язку з цим, зростаючої уваги набуває випереджальна динаміка вдосконалення системи соціальних комунікацій, основного інструменту долучення громадян до сучасних інформаційних процесів. Основну роль в окресленні нової соціальної структури цивілізації матимуть стратегічні комунікації [1], що створюють скелетну систему нових та оновлюваних інформаційних і, відповідно, соціальних систем сучасного суспільства.

Ефективність функціонування стратегічних комунікацій в умовах посилення глобальних інформаційних впливів визначає загальну стабільність соціальних структур на загальнодержавному і національному рівні, стійкість до негативних для розвитку цих структур зовнішніх інформаційних впливів, сприяє успішній реалізації державної програми інформатизації, залученню суспільно активної частини громадян до широкої участі в загальносуспільних інформаційних процесах постіндустріального суспільства.

З урахуванням даних обставин набуває додаткового значення вся система критеріїв ефективності стратегічних комунікацій України. Насамперед маємо говорити про програмно-технічне забезпечення даної системи. Рівень технічного контролю над системою, ступінь технологічної відповідності міжнародним параметрам інформаційних обмінів в усе більшій мірі в наш час визначає межі національного інформаційного простору.

Якість функціонування стратегічних інформаційних комунікацій прямо пов'язана із їх впливом на мережу всіх інших комунікацій уже наявних в національному інформаційному просторі і тих, що стрімко створюються під дією розвитку електронних інформаційних технологій. При цьому маються на увазі не лише спеціальні урядові та кризові комунікації, передбачені Доктриною інформаційної безпеки України [1], а також вся система традиційно існуючих у суспільстві комунікацій та тих, що створюються разом із вдосконалення соціальної структури суспільства у зв'язку із розвитком електронних інформаційних технологій. Процес підключення всієї цієї системи інформаційних комунікацій до стратегічних

має забезпечувати донесення найважливішої суспільнозначимої інформації всім адресатам комунікацій у мирний час. У період, коли Україна стає об'єктом зовнішньої інформаційної агресії, стратегічні комунікації мають забезпечувати також необхідний ресурс потужності для задоволення потреб ефективної відсічі інформаційному агресору в інформації оборонного та контрпропагандистського характеру.

Якість функціонування стратегічних комунікацій в значній мірі залежить від донесення користувачам змісту скоординованої державної політики, загальнонаціональних духовноціннісних орієнтирів, необхідного масиву інформації для ефективного суспільного розвитку. Зростаючого значення стратегічні комунікації набувають у зв'язку з проведенням в Україні реформ, пов'язаних із делегуванням частини економічних повноважень в регіоні [2]. Цей процес не завжди лягає на підготовлений ґрунт політико-економічної ситуації в регіонах, не завжди спирається на належну кваліфікацію професіональних спеціалістів для ефективного господарювання і нерідко проявляється в діях, що обумовлюють неефективне використання ресурсів, в тому числі інформаційних, не мобілізують місцеві інформаційні структури на ефективну співпрацю з загальнодержавним ресурсом інформації та створюють атмосферу для формування запозиченого з центру місцевого варіанту олігархату.

Активізація інформаційного впливу стратегічних комунікацій на цей процес має сприяти нейтралізації негативних збочень децентралізації. Звичайно, мова при цьому має йти про забезпечення якісного контенту для їх наповнення, підготовленого офіційними інформаційними структурами. Однак, при вирішенні масштабних завдань загальносуспільної важливості, і особливо – в умовах інформаційної війни, навіть підготовка якісної інформації з даної системи джерел не може ефективно забезпечити виконання функції інформаційної підтримки державницької діяльності без підтримки громадських структур.

В умовах розвитку інформатизації, загального доступу до наявних інформаційних ресурсів і можливостей нового інфотворення об'єктивно виникає необхідність розширювати можливості інтерактивних технологій, якісного вивчення зворотного зв'язку з групами користувачів по актуальній тематиці суспільного інформування і поступово виробляти дієві технології залучення до суспільнозначимого інфотвореннння творчого потенціалу громадян України.

Формування вітчизняних засобів протистояння в інформаційній війні передбачає і масштабні зміни інституційного ландшафту та правил гри в інформаційній сфері, що позначилось на створенні органами державної влади структур, покликаних відстоювати проукраїнські позиції, шляхом надання об'єктивної інформації про події в Україні, протидії негативним інформаційним впливам на українських громадян і дискредитації міжнародного іміджу держави. До таких, зокрема, можна віднести: Об'єднаний інформаційно-аналітичний центр «Єдина Країна», Інформаційно-

аналітичний центр Ради національної безпеки і оборони України, Український кризовий медіа-центр та ін.

У ТОП-10 організацій, які є найефективнішими в інформвійні з РФ, увійшли також громадські організації: центр "Миротворець", "СтопФейк", "Інформнапалм", "Інформаційний спротив", НАЦ "Українські студіїї стратегічних досліджень", ГО "Вільні Люди", Міжнародний інформаційний консорціум "Бастіон", Український інститут майбутнього та Центр досліджень армії, конверсії та роззброєння. У кожної організації різні методи протидії: створення інформаційних ресурсів, масові заходи, проведення інформаційних кампаній, тренінгів та ін. [3]

В цілому, напрацювання і державних, і громадських інформаційних структур постійно створюють значний інформаційний масив, що відображає найважливіші, актуальні проблеми сучасності. В узагальненому вигляді ця інформація може значною мірою підвищити змістовний рівень наповнення стратегічних інформаційних комунікацій і суттєво вплинути на рівень суспільної свідомості. У зв’язку з цим актуальною видається активізація державної організаційної діяльності в напрямі здійснення акумуляції, систематизації цього ресурсу в провідних інформаційних центрах країни, зокрема бібліотечних. Паралельно необхідна в загальнодержавному масштабі організація централізованої обробки, наукового опрацювання цього ресурсу академічними науковими установами та відповідними аналітичними структурами держави і розвиток методик донесення даного контенту сучасному користувачу.

Література

1. http://www.president.gov.ua/documents/472017-21374.
2. http://zakon5.rada.gov.ua/laws/show/994_036.
3. http://vlasno.info/blogi/3/blog-suspilstvo/item/24440-informatsiina-viina-z-rosiieiu-ukrain.

УДК 343.341

Гребенюк В.М.
доктор юридичних наук,
Національна академія Служби безпеки України

ІНФОРМАЦІЙНА ВІЙНА РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ КРАЇН БАЛТІЇ:МЕТА Й ТАКТИЧНІ ОСОБЛИВОСТІ

Метою інформаційної війни Російської Федерації проти країн Балтії є:

створення в образі Естонії, Латвії й Литви ворога та нелюда, закріплення переконаності у цьому серед російського суспільства і частини народу противника;

ідентоцид балтійських країн – заперечення їх права на існування;

підготовка підґрунтя для: переходу до «гарячої» фази шляхом «мирних» масових протестів; заморожування зони нестабільності на території країни-жертви, поширення на неї своєї юрисдикції, створення бази для поширення керованого хаосу на суміжні території.

Особливістю інформаційної війни РФ проти країн Балтії стало її підкорення задачам повернення сфер геополітичного впливу Росії; взяття реваншу в упокоренні народів, що входили до складу СРСР; створенні імперії з титульною російською нацією та асиміляцією інших націй.

Тактичними особливостями цієї війни є:

- визначення Естонії, Латвії та Литви середовищем, що підлягає перебудові Російською Федерацією; приниження сторони протиборства, звинувачення у недосвідченості та неспроможності до самостійного функціонування цих держав;

- критика євроатлантичного вектору країн Балтії, поширення інформації про насильницьке насадження цінностей Заходу, чужоземне походження ідей балтійської державності;

- звинувачення керівників та політичних сил балтійських країн у популізмі й брехливості на тлі «нескінченої низки помилок», що нібито допускаються ними;

в напрямку створення образу ворога

- номінування державного ладу країн Балтії етнократичним, ксенофобським, нацистським, антисемітським, фашистським, антидемократичним і тоталітарним;

- викривлення реальності шляхом маркування балтійців серед суб'єктів асиміляторської дискримінаційної політики щодо росіян та представників інших народів, налаштування проти них як російського суспільства, так і міжнародної спільноти;

- клеймування етнічних естонців, латвійців та литовців «нащадками фашистських карателів», «продовжувачами нацистських традицій»;

- таврування визвольних рухів цих народів колабораціоністськими, такими, що виникли внаслідок фашизації балтійських етносів, «продажності» та «жадібності» їх представників, що нібито і призвело до масового несприйняття радянської влади в минулому;

- ігнорування фактів: антирадянської спрямованості діяльності балтійських повстанців, яка була реакцією на репресивний та антинародний характер влади СРСР; тривання збройної боротьби за незалежність ще протягом десятиріччя після закінчення ІІ Світової війни, незважаючи на постійне і цілеспрямоване фізичне винищення радянською репресивною машиною, колективізацію та обмеження матеріального забезпечення повстанців; глибокої ідейності цієї боротьби та готовності її учасників до жертв задля високих цілей;

- найменування борців за незалежність країн Балтії пособниками нацистів, дезертирами, кримінальними елементами;

в ідентоциді держав Балтії

- викривлення історії у спосіб:заперечення багатовікової історії естонського, латвійського та литовського народів; фактів державотворення у минулому;визначення меж їх розвитку виключно на рівні нижчих прошарків в ієрархії російських та європейських державних утворень, що володіли Балтією;

- позбавлення балтійців права на власну історію, звинувачення у неправдивому трактуванні історії;

- заперечення життєздатності країн Балтії; віднесення їх державотворчих ідей до категорії міфів;

- формування домінувальної позиції щодо невідворотності повернення країн Балтії до російської орбіти (в інтерпретації відновлення СРСР, долучення до процесів СНД, Євразійського Союзу, обґрунтування хибності європейського вектору розвитку);

на рівні російського суспільства

- найменування Балтії, ЄС та НАТО націонал-радикальними та агресивними;

- формування російської громадської думки щодо гострої потреби формування інтенсивної присутності Російської Федерації в країнах Балтії, зовнішнього втручання у справи її країн; позиціонування РФ єдиною силою, здатною стабілізувати регіон, зобов'язаною захистити російськомовне населення Естонії, Латвії та Литви, що став об'єктом не просто витіснення, а й культурної та релігійної дискримінації, фізичного винищення на межі геноциду;

на рівні ЄС та НАТО

- нав'язування висновків щодо дискредитації цих структур країнами Балтії; переконування їх лідерів у «дикості», «некерованості» і «небезпечності» Естонії, Латвії та Литви;

в цілому на міжнародному рівні та рівні російського народу

- оголошення Європейського Союзу силою, нездатною стабілізувати «критичну» етнічну ситуацію в Балтії, з причин відсутності механізмів для цього, або через підігрування лідерам цих країн у їх «дискримінаційних діях»;

- перекладання вини за насильство щодо жертви – країн Балтії часів 40-их років минулого сторіччя безпосередньо на них у спосіб їх звинувачення в установленні авторитарно-націоналістичної державності, яка суперечила принципам облаштування цивілізованого світу та підлягала ліквідації; паралелізування тодішніх подій із сьогоденням та обґрунтування права РФ на застосування тієї ж схеми «інкорпорації» регіону.

Визначальними елементами гібридної війни РФ проти країн Балтії стали:активна участь у цьому, зокрема в інформаційних акціях проти них, учених Російської Федерації, значна політизація російської науки, розроблення її діячами механізмів розгортання керованого хаосу, підбір ними сил та засобів, прийомів та методів цієї війни залежно від чинників вразливості жертв;ведення цієї війни на рівнях:

російського суспільства з метою підготовки його членів до радикальних дій проти ворожих держав Естонії, Латвії та Литви; розпалювання національної ворожнечі, нетерпимості до латвійського, естонського та литовського народів у середовищі населення РФ;

на міжнародному рівні, аби нейтралізувати підтримку країн Балтії, відмежувати естонців, латвійців та литовців від єдиної Європи, «вимити» їх на маргінальну периферію ЄС, штучно вивести із загальноєвропейського процесу;

балтійських країн, задля їх ослаблення, поглиблення внутрішнього розколу, створення платформи до розгортання протестного потенціалу, тривалих масових заворушень, локальних конфліктів. При цьому факти дестабілізації ситуації та зовнішньої агресії видаються за суто внутрішні процеси, за заперечення причетності до цього Росії.

Література

1. Гібридна війна: Російська Федерація проти країн Балтії: огляд. вид. / упоряд. : С.Л. Фальченко, В.М. Гребенюк. – Київ : Нац. акад.. СБУ, 2018. – 164 с.

2. Воротніков В.В. ПрибалтийскиеэтнократиимеждуРоссией и Европой: поиск-консенсуса в условияхэкономическогокризиса. [Електронний ресурс]. – Режим доступу: http://vestnik.mgimo.ru/razdely/mezhdunarodnye-otnosheniya/pribaltiyskie-etnokratii-mezhdu-rossiey-i-evropoy-poisk.

3. Бузаев В.В. Современная европейская этнократия. Нарушение прав национальных меньшинств в Эстонии и Латвии / В.В. Бузаев, И.В. Никифоров. – М., Фонд «Историческая память». – 2009. – 280 с.

4. Гапоненко О.В. Этническиеконфликты в странахБалтии. [Електронний ресурс]. – Режим доступу: http://www.perspektivy.info/history/etnicheskije_konflikty_v_stranah_baltii_2008-12-12.htm.

5. Розенбанд А.Й. «Демократия булыжников» в Прибалтике.[Електронний ресурс]. – Режим доступу: http://www.perspektivy.info/print.php?ID=36164.

6. Розенбанд А.Й. О мифах в эстонскойполитике и историографии. [Електронний ресурс]. – Режим доступу:http://www.perspektivy.info/history/o_mifah_v_estonskoj_politike_i_istoriografii_2007-05-20.htm.

УДК: 316.485.6:351.746.1(477)
Давиденко М.О.
кандидат юридичних наук,
Національна академія СБ України

ПРОТИДІЯ СБ УКРАЇНИ ТЕРОРИСТИЧНІЙ ПРОПАГАНДІ У ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ УКРАЇНИ

З метою систематичної підтримки терористичної діяльності т.зв. «ДНР»/«ЛНР» та зважаючи на низьку результативність застосування засобів традиційної війни у 2015-2016 рр., спецслужбами РФ спільно з науково-статистичними центрами планується та проводиться широкомасштабна інформаційна пропаганда та поширення ідеології тероризму як на окупованій території, так і прилеглих до лінії розмежування населених пунктах та стратегічно важливих для держави-агресора регіонах, зокрема: Харківській, Запорізькій, Дніпропетровській та Херсонській областях тощо.

Юридична енциклопедія дає наступне визначення пропаганди (*від лат. propagare – поширювати, розповсюджувати*) – діяльність, що передбачає систематичне поширення, поглиблене роз'яснення соціально-політичних, економічних, правових поглядів, ідей, теорій та забезпечує формування у суспільстві певних настроїв, закріплення у свідомості громадян тих чи інших цінностей, орієнтацій, уявлень з метою максимального розширення кола прибічників відповідно ціннісної системи [1, с. 166].

Так, основні тематичні напрями здійснення терористичної пропаганди т.зв «ЛНР»/«ДНР» можемо розділити на такі блоки:

1. Перший, спрямований на населення підконтрольних територій з метою: виправдання правомірності утворення квазі-республік та анексії АР Крим; створення у населення позитивного відношення до т.зв. «ЛНР»/ «ДНР».

2. Другий – «романтизація» бойовиків, створення образу «визволителів», порівняння з солдатами Великої Вітчизняної війни; поширення антиукраїнських матеріалів, псевдо-фактів та фейкових матеріалів про кризові процеси в українській армії (алкоголізм, мародерство, дезертирство, непрофесіоналізм тощо).

3. Третій – спрямований на пошук і залучення молоді до молодіжних воєнізованих таборів на кшталт «Молодая гвардия» (Православная организация им. Г. Победоносца), «Молодая республика», «Патриоты Донбасса» та інші.

4. Четвертий – відеоматеріали та новини для нагнітання страху, призиви до знищення «укропів та укрів», здійснення терактів на території України, знищення українських солдат, показ страт вояків тощо.

Можемо засвідчити, що основна тематична пропаганда здійснюється на сайтах: «Youtube» (відео канал «ДНР/ЛНР»), «news-front.info», «rus-vesna.su», «dnr24.com», «dnr-news.com» і тд.

Антитерористична пропаганда СБ України здійснюється через систему взаємоузгоджених заходів, які застосовуються комплексно. Основними з них є:

1. Інформаційно-пропагандистська діяльність органів влади та правоохоронних структур.

Дана діяльність має полягати перш за все у попередженні виникнення умов для здійснення терористичної пропагандистської діяльності, адекватному реагуванню на спроби розповсюдження терористичної ідеології, викриття фейкових матеріалів.

2. Розвінчування ідеології тероризму (його антологічних і гносеологічних основ).

На наш погляд, СБ України за підтримки низки медіа-ресурсів, журналістів мають готуватися доступні для молоді матеріали, які стосуються негативних наслідків терористичної діяльності. Вважаємо, що документальні фільми та наукові конференції не будуть відігравати великої ролі серед молодіжного середовища.

3. «Деромантизація» терористичних лідерів.

Дослідники схиляються до такого тлумачення поняття «деромантизація» – це дискредитація ідеалів, цінностей вищого порядку, у тому числі представлених в думках, поглядах, гаслах, протиставлення їм грубо утилітарного, цинічного відношення до дійсності [2].

Зауважимо, що «деромантизація» лідерів терористичних угруповань СБ України має здійснюватись, перш за все, у молодіжному середовищі як одним із елементів роботи оперативного співробітника.

4. Контроль і протиборство з ідеологією тероризму у мережі Інтернет (блокування сайтів, публікацій на форумах, соціальних мережах).

5. Організація інформаційного контролю за середовищем молоді.

Таким чином, схиляємося до думки, що антитерористична пропаганда – це елемент державної антитерористичної стратегії, який являє собою багаторівневу систему правил, теорій, поглядів, переконань і установок, які доводяться до громадян через систему гласних та негласних заходів як з метою протидії пропаганді та поширенню ідеології тероризму так і виховання і формування у кожного члена суспільства неприйнятного ставлення до терористичної діяльності, антиекстремістського світогляду, максимального розширення кола прибічників антитерористичної ідеології.

Література

1. Юридична енциклопедія // В 6 т. /Редкол.: Ю.С. Шемшученко (голова редкол.) та ін. – К.: “Укр. енцикл. ”, 1998 – Т. 5: П-С. – 2003. – С.166-167.

2. Кара-Мурза С.Г. Манипуляция сознанием / С.Г. Кара-Мурза [Электронный ресурс]. – Режим доступа : http: //www.ru / polittech /121817/ se_index.

УДК 355.01 : 378.016
Даниленко В. М.
доктор історичних наук, професор,
Національна академія Служби безпеки України

ВУЗЛОВІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВИВЧЕННІ ДИСЦИПЛІН ГУМАНІТАРНОГО ЦИКЛУ

Гібридна війна, розв'язана Росією проти України, загострила необхідність напрацювання гнучкого комплексного підходу до вивчення предметів і явищ об'єктивної дійсності, де не може бути місця для догм і закостенілості форм і методів навчання. Очевидно, що в наш час доцільно максимально наближувати його зміст до практичних потреб забезпечення інформаційної безпеки людини, держави, суспільства.

За традицією майбутні фахівці з інформаційної безпеки акцентують увагу головно на технічній складовій навчання. Водночас якісні характеристики професійних компетентностей значною мірою залежать також від рівня засвоєння дисциплін гуманітарного циклу. Як відкриття нових процесів і явищ нерідко відбуваються на стику різних галузей наук, так і оригінальні знання формуються сукупністю інформації, яка надходить з різних джерел. Юристи, філологи чи історики прямо не ведуть боротьби з інформаційною агресією противника, проте вони готують матеріал для підготовки осіб, здатних орієнтуватись у технічній, військовій та гуманітарній сферах і ефективно реалізовувати покладені на них суспільством завдання.

Серед дисциплін гуманітарного циклу, роль яких у інформаційному протиборстві може бути посилена, виділимо такі, як філософія, право, історія України, історія української культури, політологія, українська ділова мова, релігієзнавство, етика, психологія.

У багатьох випадках інформаційні атаки противника ведуться з розрахунку на заангажованість аудиторії, наявність прогалин у підготовці, некомпетентність споживачів інформації. Вбачається, що на сьогоднішній день важливо вже на ранніх етапах навчання прищеплювати й розвивати у здобувачів освіти стійкий імунітет до зовнішніх загроз гуманітарного характеру, а це можна зробити тільки через поглиблення наукових знань. Виклики так чи інакше потребують адекватного реагування в інформаційному просторі. Відповіді на них будуть ефективними й досягнуть мети при наявності вагомих контраргументів, документальних доказів, наявності внутрішніх переконань.

Одним із вузлових є питання «русского мира», яке неможливо однозначно трактувати, проте воно активно використовується керівництвом РФ для нав'язування власної великоімперської ідеології і поширення свого впливу серед російськомовного населення на пострадянському просто-

рі. Концепт «русский мир»» має практичним наслідком розв'язування воєнних дій в Україні і готовність до застосування сили в інших регіонах планети. Перформативність вибудуваних на цій основі концепцій, які використовуються для досягнення глобальних цілей, потребує філософського переосмислення наявних ідеологем і встановлення їхнього зв'язку з попередніми етапами зовнішньополітичної експансії Росії. В інформаційній війні тут не обійтись без ґрунтовних знань з питань мови, релігії, історії політичних вчень і міжнародних відносин.

Вузловим питанням для міжнародного права,політології й історії є пошуки інформаційних ресурсів та вдосконалення мультимедійних засобів для переконання аудиторії, на яку розрахована риторика опонентів, у згубності егоїстичної політики російської влади і доведення відсутності в історії людства розумної альтернативи мирному співіснуванню й демократичному розвитку народів. Сценарії «нелегітимності» влади в Україні, неспроможності державного будівництва, які постійно розробляють і намагаються інфікувати в українське суспільство російські пропагандисти, важливо спростовувати ще в процесі вивчення дисциплін гуманітарного циклу.

У сферу інформаційної безпеки потрапляють питання боротьби за культурну спадщину і духовну емансипацію українського народу, релігійні чинники стабільності суспільства. Протягом століть український народ створив оригінальну культуру, яка стала невід'ємною частиною світової. Багатовікове входження українських земель до складу інших країн, бездержавність одного з найчисленніших європейських народів призвели до затягування вузла питань, пов'язаних із національною ідентифікацією українців і розбудовою власної суверенної держави. Вивчення суперечливих і гострих питань походження української мови, формування нації, історії й культури українського народу, його взаємин з іншими народами є запорукою нарощування знань, що згодом можуть стати основою для гідної відповіді на виклики новітнього часу.

Таким чином, у сфері забезпечення інформаційної безпеки відкривається широке поле для прийняття креативних творчих рішень. У цьому контексті важливим є висвітлення низки тем дисциплін гуманітарного циклу крізь призму новітньої інформаційної війни, кадри для якої з російської сторони, очевидно, готувалися заздалегідь. Вузловим питанням підготовки фахівців у галузі інформаційної безпеки є, на нашу думку,привернення їхньої уваги до тих розділів дисциплін, поглиблене вивчення яких найімовірніше може знадобитися у відверненні недружніх, а то й ворожих акцій, організованих проти України. Щоб працювати на випередження, потрібно знати потенційні загрози для безпеки держави, їх соціальну спрямованість, причинно-наслідкові зв'язки, володіти методами локалізації, нейтралізації й ліквідації таких загроз. Успіх у цій справі залежить від оперативності опрацювання передбачених навчальними планами тем не тільки з освітньою чи пізнавальною метою, але й як один із напрямів забезпечення інформаційної безпеки.

УДК 007:351.861
Довгаль Ю.С.
Міжвідомчий науково-дослідний центр
з проблем боротьби з організованою злочинністю
при РНБО України

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Відповідно до фундаментальних положень Доктрини інформаційної безпеки України забезпечення інформаційного суверенітету, запобігання інформаційній агресії, експансії та інформаційній блокаді України з боку іноземних держав, організацій, груп та осіб є пріоритетним завданням політикуму нашої країни. Інформаційна безпека держави є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз і являє собою сукупність інформаційно-психологічної (психофізичної) та інформаційно-технологічної безпеки держави[1].

Актуальністю даної теми є те, що важливою змістовною складовою національної безпеки є інформаційна безпека. Із зростанням науково-технічного прогресу буде зростати і важливість питання інформаційної безпеки громадянина, суспільства, держави. Тобто інформація стала чинником, який може призвести до значних технологічних аварій, військових конфліктів та поразок у них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів, і чим вищий рівень інтелектуалізації та інформатизації суспільства, тим потрібнішою стає надійна інформаційна безпека, оскільки реалізація інтересів, людей та держав все більше здійснюється за допомогою інформатизації. Враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися кругозір та мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів скритого агресивного впливу, виявлення дій, що мають цілеспрямований агресивний характер і які протирічать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах [2].

Інформаційна безпека - стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження,

використання і порушення цілісності, конфіденційності та доступності інформації.

Вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

В Україні політика забезпечення інформаційної безпеки будується на таких засадах:

обмеження доступу до інформаційного ресурсу є винятком із загального принципу відкритості інформації й реалізується тільки відповідно до чинного законодавства;

суб'єкти, які збирають, накопичують і обробляють персональні дані й конфіденційну інформацію, несуть відповідальність перед законом за збереження і використання;

держава забезпечує захист суспільства від хибної, викривленої і недостовірної інформації, що надходить через засоби масової інформації;

держава реалізує контроль за створенням і використанням засобів захисту інформації шляхом їхньої обов'язкової сертифікації та ліцензування діяльності в галузі захисту інформації;

держава сприяє всебічному розвитку української мови як основного інструменту перетворення накопичених людством знань в інформаційний ресурс України [3].

З урахуванням майбутнього розвитку інформатизації, проникнення інформаційних технологій у найважливіші сфери життя суспільства необхідно передбачити перехід від принципу забезпечення безпеки інформації до принципу інформаційної безпеки. Розгляд інформаційної безпеки з позицій системного підходу дозволяє побачити відмінність наукового розуміння цієї проблеми від повсякденного. В повсякденному житті інформаційна безпека розуміється лише як необхідність боротьби з відтоком закритої (таємної) інформації, а також з розповсюдженням хибної та воро-

жої інформацій. Осмислення нових інформаційних безпек у суспільстві ще тільки починається [4].

Отже, інформаційна безпека суспільства, держави характеризується ступенем їх захищеності, та, як наслідок, стійкістю головних сфер життєдіяльності у відношенні до небезпечних інформаційних впливів. Інформаційна безпека визначається здатністю нейтралізувати такі впливи. Загальноприйнятим є таке визначення інформаційної безпеки, як стан захищеності життєво важливих інтересів громадян, суспільства та держави в інформаційній сфері.

Література

1. Доктрина інформаційної безпеки України: Затверджена Указом Президента України від 25 лютого 2017 року № 47/2017. URL: http://zakon.rada.gov.ua/laws/show/47/2017?lang=ru.

2. Лужецький В.А. Інформаційна безпека: навч. посіб. / В.А.Лужецький, О.П.Войнович, А.В.Дудатьєв. – Вінниця : УНІВЕРСУМ-Вінниця, 2009. – 240 с.

3. Роговець В. Інформаційні війни в сучасному світі: причини, механізми, наслідки / В.Роговець // Персонал. – 2000. – № 5.

4. Комп'ютерна злочинність і інформаційна безпека / А.П.Леонов; під заг. ред. А.П.Леонова. – Мінськ: АРІЛ, 2000. – 552 с.

УДК 340+35.078.3

Довгань О.Д.
доктор юридичних наук,
старший науковий співробітник,
заслужений діяч науки і техніки України,
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

ЩОДО ДЕЯКИХ АСПЕКТІВ НЕОБХІДНОСТІ СТАНОВЛЕННЯ І РОЗВИТКУ НАЦІОНАЛЬНОЇ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Поступове зміщення центру ваги вирішення спірних та конфліктних питань на всіх рівнях в інформаційний простір створили нові виклики і загрози в інформаційній сфері.

В таких умовах, протягом останніх років в Українському суспільстві спостерігається тенденція до все більшого розуміння важливості проблем розвитку інформаційної сфери та необхідності забезпечення інформаційної безпеки в усіх сферах життєдіяльності людини, суспільства і держави. Оскільки, актуальними постали питання формування цілісної системи забезпечення інформаційного суверенітету, управління ризиками і можли-

востями новітніх викликів в інформаційній сфері, розбудови власних спроможностей і стратегічних комунікацій тощо.

Це насамперед пов'язано з процесами, що відбуваються в глобальному інформаційному просторі і характеризуються такими основними тенденціями та особливостями:

глобальні зміни і трансформації в інформаційній сфері формують новітні виклики і загрози, які становлять реальну загрозу безпеці людства та міжнародному правопорядку;

в інформаційному просторі спостерігається тенденція до поширення інформаційної агресії і насилля, маніпуляції свідомістю людини та суспільства, періодично проводяться інформаційно-психологічні операції;

більшість країн світу зіштовхнулася з проблемами кібершпигунства, кібертероризму, кіберзлочинності та кібератаками на об'єкти критичної інфраструктури;

наслідки використання сучасної інформаційної зброї можуть призводити до реальної втрати державного суверенітету і територіальної цілісності країн світу.

Тому, з боку держави повинні вживатися відповідні дії з адекватного реагування на такі загрози і в першу чергу, з використанням правових механізмів, спираючись на вимоги ст. 17 Конституції (*забезпечення інформаційної безпеки є однією з основних функцій держави і справою всього Українського народу)* та законів України.

Крім того, потребують першочергового вирішення завдання у сфері забезпечення інформаційної безпеки і захисту прав людини в інформаційній сфері та вжиття відповідних заходів пов'язаних зі становленням та розвитком системи інформаційної безпеки, а саме:

удосконалення державної інформаційної політики та політики інформаційної безпеки, належного правового, організаційного, науково-технологічного, кадрового та іншого ресурсного забезпечення її реалізації;

розвитку національної системи кібернетичної безпеки, згідно з прийнятими нормативно-правовими актами і стандартами країн-членів ЄС і НАТО. Насамперед, це стосується захисту об'єктів критичної інфраструктури, державних реєстрів і баз даних;

опрацювання правових, організаційних, технічних та інших питань протидії інформаційному насиллю та використанню мереж соціальних комунікацій на шкоду людині, суспільству і державі;

розгляду питання щодо переведення системи протидії інформаційній агресії проти України в режим «активної інформаційної оборони», насамперед, щодо запобігання нанесення шкоди життю і здоров'ю людини та захисту національних інтересів;

організації належного захисту прав, свобод і безпеки людини в інформаційній сфері, насамперед, відповідно до GDPR "Пакету захисту даних" ЄС, який набув чинності у травні 2018 року, і запровадив такі базові принципи роботи з персональними даними: законність, справедливість,

прозорість, цільове обмеження, зведення до мінімуму даних, точність, обмеження терміну зберігання, цілісність і конфіденційність.

Для створення належних умов реалізації державної політики, спрямованої на захист національних цінностей та реалізацію національних інтересів України, гарантування безпеки особи, суспільства і держави від зовнішніх та внутрішніх загроз в інформаційній сфері, потребує формування сучасних ефективних механізмів забезпечення інформаційної безпеки, які відповідатимуть характеру і масштабам викликів сьогодення. Сама ж система інформаційної безпеки має бути спрямована на ефективний захист об'єктів національної безпеки: людини і громадянина – їх конституційних прав і свобод; суспільства – його духовних, морально-етичних, культурних, історичних, інтелектуальних та інших цінностей; держави – її конституційного ладу, суверенітету, територіальної цілісності й недоторканності.

Література

1. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних/ Збірник документів ; [неофіційний пер. з англ. І. Майстренко; за ред. В.Брижко; передмова В.Пилипчука]. - (Науково-дослідний інститут інформатики і права Національної академії правових наук України). - К. : ТОВ "Видавничий дім "АртЕк", 2018. 180 с.

2. Довгань О.Д. Система інформаційної безпеки України: онтологічні виміри/ О.Д. Довгань, Т.Ю.Ткачук // Інформація і право № 1 (24). 2018 . С. 89-103.

3. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К.: Видавничий дім «АртЕк», 2018. №1-12.

УДК 342.53:004(477)

Дорогих С.О.
кандидат юридичних наук,
старший науковий співробітник,
Науково-дослідний інститут
інформатики і права НАПрН України

ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ ВЕРХОВНОЇ РАДИ УКРАЇНИ В КОНТЕКСТІ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ

Починаючи з 2014 року Україна стала ціллю військової агресії з боку Російської Федерації. Ще раніше (фактично від часів незалежності) РФ почала завдавати постійних інформаційних нападів на Україну, піддаючи

сумніву сам сенс існування України як суверенної та незалежної держави, а також українського народу як такого.

Одним з напрямів таких інформаційних нападів є дискредитація системи влади в Україні, приниження її досягнень та гіперболізація недоліків, спотворення реальної картини й, нарешті, створення різноманітних фейків.

В таких умовах відкритість та прозорість діяльності влади, залучення громадян до прийняття управлінських рішень є однією ланок захисту в умовах інформаційної агресії.

Принципи відкритості та прозорості закладено серед парламентських цілей та цінностей, яким повинен слідувати український парламент.

Шляхи досягнення поставлених цілей та цінностей було визначено у низці документів, до яких приєдналася Верховна Рада України і на виконання яких, були прийняті власні документи.

5 липня 2012 року була прийнята Програма інформатизації законотворчого процесу у Верховній Раді України на 2012-2017 роки, яка ставила за мету досягнення максимально можливої автоматизації інформаційно-організаційних процесів у діяльності депутатського корпусу загалом, у тому числі комітетів Верховної Ради України, депутатських фракцій, а також Апарату Верховної Ради України шляхом створення сучасних систем управління законотворчим процесом та документообігом у парламенті.

17 березня 2016 року було прийнято Постанову Верховної Ради України «Про заходи з реалізації рекомендацій щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України». У постанові перелічені ряд заходів й щодо питань електронного парламентаризму, зокрема:

– Необхідно розробити та схвалити стратегію переходу до електронного парламентаризму, включаючи середньострокову стратегію Інформаційних та Комунікаційних технологій (на 3-5 років). Слід передбачити відповідні ресурси, спрямовані на підвищення рівня прозорості та ефективності парламентських процесів.

– Верховна Рада України повинна розробити та схвалити "цифрову" стратегію, яка б дала змогу створити сучасну службу з питань Інтернету та соціальних медіа із залученням команди досвідчених експертів з метою підвищення популярності он-лайн платформи Верховної Ради України.

– Верховна Рада України повинна розробити та схвалити всеохоплюючу комунікаційну стратегію (з визначенням основних аудиторій, каналів донесення інформації та інформаційних продуктів) та брендингову стратегію інституції, яка б визначала довгострокові цілі у здійсненні комунікаційної політики, визначенні характеру комунікації та інформаційних сигналів.

У лютому 2016 року Верховна Рада України приєдналася до Декларації відкритості парламенту.

Декларація визначає чотири основні напрями роботи:

– просування культури відкритості;
– забезпечення доступності інформації про діяльність парламенту;
– полегшення доступу до інформації про діяльність парламенту;
– забезпечення доступу до інформації про роботу парламенту в електронному вигляді.

Відтак ВРУ через свій офіційний сайт намагається представити найрізноманітнішу інформацію щодо роботи парламенту, починаючи з повністю відкритих безкоштовних баз нормативно-правових актів та законопроектів. Так само громадянам надано право відвідувати засідання парламенту, таким чином, можна констатувати, що процес просування культури відкритості наближається до світових стандартів.

Політика відкритості та прозорості інформації про діяльність парламенту передбачає, що парламент повинен прийняти курс на забезпечення активної публікації інформації про діяльність парламенту.

У листопаді 2017 року відбулася презентація Комунікаційної стратегії Верховної Ради України на 2017-2021 роки, спрямована на підвищення рівня довіри до Верховної Ради України та сприйняття її як ефективної інституції серед громадян України, організацій громадянського суспільства, засобів масової інформації та міжнародних аудиторій.

Запропонована п’ятирічна комунікаційна стратегія Верховної Ради України доповнює План дій з реалізації відкритості парламенту і ставить за мету посилення інституційної спроможності Верховної Ради України, здійснення сучасного, повного та неупередженого інформування про діяльність Верховної Ради України у впровадженні демократичних перетворень та зміцнення позитивного іміджу парламенту.

УДК 343.1

Злагода О.В.
кандидат юридичних наук,
Національна академія внутрішніх справ

ДЕЯКІ ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНАХ ТА ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

За останні роки в Україні спостерігається загострення криміногенної обстановки. В зв’язку з посиленням боротьби зі злочинністю, збільшився потік інформації, що обробляється правоохоронними органами, зросла кількість оперативних документів, які потребують негайного вирішення. Значно зріс обсяг існуючих банків даних, які досягли тієї межі, коли наявні технічні засоби та технології не дозволяють оперативно та якісно обробляти інформацію, що надходить.

Слід зазначити, що кожна держава повинна захищати свою незалежність, територію, інтереси свого народу, громадян, інтереси економіки тощо. Держава є власником певної інформації, що не може бути розголошена у широкому загалі.

Згідно статті 20 Закону України «Про інформацію» інформація за порядком доступу поділяється на відкриту та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. Інформація з обмеженим доступом є конфіденційна, таємна та службова інформація [1].

Інформаційна безпека в органах Національної поліції України полягає у збереженні цілісності інформації, що циркулює в поліції, і має свої особливості. В першу чергу це стосується інформації, що містить державну таємницю.

Відзначимо, що державна таємниця – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані державною таємницею та підлягають охороні державою[2, с. 7].

Перелік відомостей, що містять державну таємницю, відзначена у «Зводі відомостей, що становлять державну таємницю»,затверджено наказом СБУ від 12.08.2005 р. № 440[3].

Крім того захисту потребує конфіденційна інформація в автоматизованих системах, каналах електрозв’язку та у робочих приміщеннях підрозділів Національної поліції України. Правоохоронні органи потребують також захисту від дезінформації.

Безпека та захист в інформаційній системі має будуватися з урахуванням комплексного підходу до побудови системи захисту, що передбачає об’єднання в єдиний комплекс необхідних заходів та засобів захисту інформації на всіх рівнях системи інформаційного забезпечення.

Слід врахувати, що система інформаційної безпеки в органах Національної поліції України ґрунтується на положеннях норм Законів України «Про захист інформації в автоматизованих системах», «Про захист інформації в інформаційно-телекомунікаційних системах», а також Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 року № 1229/99, Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджене постановою КМ України від 16 лютого 1998 року № 180 [4-7].

Система інформаційної безпеки має бути спрямована на запобігання втрати інформації, їй спотворення, несанкціонованого доступу та неза-

конного її використання на етапах проектування, впровадження та експлуатації інформаційних підсистем.

Безпека інформації повинна забезпечуватися на технологічних рівнях збору, накопичення, обробки та передачі інформації.

Підводячи підсумок, слід зазначити, що аналіз роботи органів та підрозділів Національної поліції свідчить, що однією з проблем попередження, виявлення та розкриття злочинів є недостатній рівень захищеності відомчих інформаційних мереж та систем, доступ до інтегрованих інформаційно-пошукових систем і баз.

Це в свою чергу, пояснюється серйозними вадами існуючої системи збору, обробки та обміну інформацією між органами та підрозділами Національної поліції України.

Література

1. Про інформацію: Закон України від 2.10.1992. База даних «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua//зі змінами від 6.12.2016р. (дата звернення 3.03.2019)

2. Інформаційна безпека правоохоронних органів: Курс лекцій / О.В. Рибальський, В.Г. Хахановський, Ю.Ю. Орлов та ін.. – К.: Нац. акад. внут. справ, 2004.-148с.

3. Про затвердження Зводу відомостей, що становлять державну таємницю: Наказ СБУ від 12.08.2005 №440. База даних «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua //зі змінами від 16.11.2018р. (дата звернення 3.03.2019 (дата звернення 3.03.2019)

4. Про захист інформації в автоматизованих системах Закон України від 31.05.2005. База даних «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua(дата звернення 3.03.2019)

5. Про захист інформації в інформаційно-телекомунікаційних системах Закон України від 5.07.1994. База даних «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua //зі змінами від 27.03.2014р. (дата звернення 4.03.2019)

6. Положення про технічний захист інформації в Україні, затверджене указом президента України від 27 вересня 1999 року №1229/99. База даних «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua// зі змінами від 4.05.2008р. (дата звернення 4.03.2019)

7. Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах затверджене постановою КМ України від 16 лютого 1998 року №180. База даних «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua(дата звернення 4.03.2019)

УДК 316.77: 614.8.014
Золотар О.О.
доктор юридичних наук,
старший науковий співробітник,
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

ПРОПАГАНДА В СОЦІАЛЬНИХ МЕРЕЖАХ – ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ

З кожним роком суспільство занурюється в соціальні мережі. Кількість часу, що пересічна людина проводить в соцмережах з 2012 року зросла вдвічі і в 2019 році становить 2 години 22 хв[1]. Більше часу людина проводить лише перед екраном телевізора. Тому відповідно саме ці два канали інформаційних впливів і стали полями для розгортання пропагандистських операцій.

Поняття «пропаганда» має витоки у католицизмі, походить від назви створеної у 1622 році Конгрегації *поширення* віри, яка латинською звучала як Congregatio de *Propaganda* Fide. Корінь «*propago*» перекладається не лише як дієслово «поширювати», а також як іменники «розмноження», «нащадок, потомство»[2]. Власне, останні розуміння, зараз як інколи актуалізуються в соцмережах, оскільки переважна кількість користувачів (близько 90%) лише поширює і коментує, тобто творить нову інтерпретацію тієї ж новини чи події.

Рівень усвідомленості загрози інформаційній безпеці держави, яку становить пропаганда в соціальних мережах, суттєво відрізняється в різних країнах світу. Проте дослідження можливостей інформаційних впливів за допомогою нових медіа, в тому числі соціальних мереж здійснюються в багатьох країнах світу – наприклад, США, Сполученому Королівстві, ФРН, КНР, Російській Федерації, та інших державах. При цьому дослідження здійснюються в багатьох наукових напрямках – національна безпека; політичні, економічні, юридичні, військові, соціологічні, медичні та психологічні науки, інформатика і кібернетика, журналістика і соціальні комунікації, державне управління та, навіть, мистецтвознавство і філологія. Зокрема, при підготовці цього виступу було використано праці А. Герна, Г. Почепцова, А. Петленда і П. Померанцева.

В чому ж саме специфіка пропаганди в соціальних мережах і чим вона відрізняється від своїх попередників – друкованої пропаганди, радіо- і телепропаганди?

---

[1] https://www.digitalinformationworld.com/2019/01/how-much-time-do-people-spend-social-media-infographic.html.

[2] Latin English Dictionary online https://glosbe.com/la/en/propago.

Міжперсональна комунікація або «всі для всіх». Попередні покоління медіа використовували горизонтальну модель впливу, коли власник або інший суб'єкт визначав основний зміст наративу, що доносився до об'єктів пропагандистського впливу – читачів, слухачів, глядачів. Як правило, суб'єкти впливу були стабільні і ідеологія, що пропагувалась ними, була однотипною для невизначеного кола осіб. Що при наявності альтернативних джерел інформації і здібностей до критичного сприйняття інформації давало можливість виявити і протидіяти пропаганді.

Соціальні медіа мають горизонтальну структуру з багатьма гравцями, що використовують різні тактики і мають різні цілі впливу. Таким чином, створюється **ілюзія поінформованості**, користувачеві здається, що всі про це пишуть/говорять/знають і ця інформація надійшла від невизначеного кола осіб. Цим успішно користається російська пропагандистська машина. В доповіді Ради Європи «Боротьба з дезінформацією в глобальній медіамережі» підкреслюється, що одночасно тисячі інтернет-джерел використовуються для поширення прокремлівської дезінформації в соцмережах, а разом вони створюють враження нібито незалежних джерел, що підтверджують повідомлення один одного.

«Інформаційна бульбашка» або «кредит довіри». Особливості поширення інформації в соцмережах - швидкість комунікаційного обміну, відсутність просторово-часових обмежень, позірна масштабність аудиторії, фільтрація інформації – посилюють вплив на користувача. Повідомлення в соцмережах поширюються на сторінках медіаресурсів, за якими користувач *обрав* стежити; шляхом розсилки новин від спільноти, до якої користувач долучився за *власним вибором*, або ж безпосередньо від користувача до користувача, який є другом або фоловером. З психологічної точки зору користувач сприймає свою сторінку як особистий простір, що обумовлює апріорі вищий рівень довіри до одержуваної в мережі інформації, ніж з інших джерел. Таким чином, за допомогою алгоритмів соцмереж користувач поміщується у визначені ідеологічні рамки.

«Тролі/боти і інші потвори...» або бізнес на політиці. Високий ступінь технологізації пропаганди в соцмережах дозволив комерціалізувати цю діяльність і перетворити в прибутковий бізнес. Політтехнологи, пропагандисти, піарщики і маркетологи в сучасних умовах стали представниками одного «цеху». В 2018 році та за кілька місяців цього року основні гравці – Твітер, Фейсбук і Ютюб неодноразово оголошували про видалення численних фіктивних аккаунтів, або як це культурно назвали в своєму пресрелізі Фейсбук – «координовану неавтентичну поведінку». Ботоферми і тролі – це вже давно не поодинокі гравці, а сегментований і професійний ринок послуг зі значною конкуренцією, де одні – створюють фіктивні аккаунти, другі – імітують їх активність, треті – здійснюють регулярні вкидання підготованої інформації, а ще інші – пишуть маніпулятивні тексти, творять фейкові фото та відео...

Соціальний тиск або «ефект віртуального натовпу». А. Пентленд стверджує, що соціальні мережі впливають на людей вчетверо сильніше, ніж традиційний індивідуальний підхід, який використовується в маркетингу.

Вплив пропаганди в соціальних мережах залишається малодослідженою загрозою інформаційній безпеці держави, що не дозволяє повною мірою ані його спрогнозувати, ані адекватно протидіяти.

Література

1. Pentland A. Social Physics: how good ideas spread — the lessons from a new science. Scribe Publications Pty Limited, 2014. 320 p.

2. Hern A. Facebook and Twitter are being used to manipulate public opinion – report. URL: www.theguardian.com/technology/2017/jun/19/social-media-proganda-manipulating-public-opinion-bots-accounts-facebook-twitter

3. Pomerantsev P. Why we're post-fact? URL: https://granta.com/why-were-post-fact/

4. Почепцов Г. Пропаганда 2.0. Харків, Фоліо, 2018. 800 с.

УДК 351.746.1

Іванов О.Ю.
кандидат юридичних наук,
Національна академія Служби безпеки України

КОНЦЕПТ «РУССКИЙ МИР» У РОСІЙСЬКІЙ ПРОПАГАНДІ: БАЛКАНСЬКИЙ ВЕКТОР

Історичний складник відіграє вкрай важливу роль у підтриманні ідеологічного впливу Російської Федерації (далі – РФ) на балканські країни на сучасному етапі. Зокрема, поширеною є практика створення в них російських культурних центрів, представництв, громадських організацій, діяльність яких оголошується базованою на необхідності підтримання історично сформованих зв'язків між російським і сербським, болгарським, грецьким та іншими народами. Так, наприклад, у Болгарії діють такі організації, як «Російський академічний союз у Болгарії» та Фонд «Русский мир». У 2009 р. ними здійснено спільне видання книги-альбому під назвою «Російське зарубіжжя в Болгарії: історія та сучасність», у передмові до якого зазначалося, що це «...унікальна книга-альбом, у якій Російське зарубіжжя [авторську орфографію збережено – О.І.] в цій країні... розглядається як єдиний історичний процес та явище за майже двохсотрічну історію...» [1]. Відтак, із самого початку автори видання чітко вказали на історичні зв'язки між росіянами та болгарами, приховано підкресливши давні експансіоністські прагнення Росії.

Наповнений історичним контекстом також і термін «російське зарубіжжя», зміст котрого не можна звести лише до культури повсякденного життя російських емігрантів у Болгарії. У цьому випадку хоч і завуальовано, але першочергово йдеться про збереження російського впливу через діяльність культурних організацій, а також про підтримання нав'язаних іще російськими військовими переселенцями в ході російсько-турецьких воєн XIX ст. традицій. Сама діяльність відповідних культурних центрів також підпадає під означення російського зарубіжжя. Автори книги-альбому також зазначають, що вона «... розрахована на... російських співвітчизників у Болгарії... і адресована всім тим, для кого є дорогими історія російського зарубіжжя та його духовний спадок», тим самим підкреслюючи нібито важливість впливу російської культури на формування болгарської, а також його глибинні історичні витоки. Незначна частка росіян в етнічному складі населення Болгарії також ставить під сумнів правдивість тих намірів, які декларують російські культурні центри в цій країні. У виданні історія становлення офіційних російсько-болгарських відносин (дипломатичних, культурних, політичних) подається починаючи зі встановлення радянської влади в Росії в 1917 р., аналогічні ж процеси за часів Російської імперії майже повністю залишаються поза увагою укладачів аналізованого видання.

Одна із рубрик книги-альбому має назву «Шляхи адаптації і самозбереження «русского мира» [лапки наші, автентичність терміну збережено – О. І.] в Болгарії (1920-і рр.)»[1, с. 146–148]. Автор рубрики З. Бочарова стверджує про близькість російського та болгарського народів із таких підстав: конфесійна спорідненість, схожість культур, мов та законів Російської імперії і Болгарії. Втім, відсутні будь-які згадки про те, за рахунок чого, у який спосіб і коли сформувалася така показна схожість цих двох етносів. Причому статус етнічних росіян у Болгарії визначається в якості біженців, котрі після розпаду імперії Романових змушені були тікати, а на чужині тепер зазнавали утисків. У тексті звучить непрямий заклик до сучасного болгарського уряду продовжувати розпочаті їх попередниками традиції прихильного ставлення до етнічних росіян і сприяння розвитку їхньої культури. З. Бочарова описує неприязну політику болгарського уряду щодо росіян на початку 1920-х рр., не зазначаючи про витоки її передумов у характері політики царської Росії щодо Болгарії. Загальний контекст розділу зводиться до того, що розгортання діяльності російських культурних організацій на території цієї країни стало можливим нібито через відновлення місцевим урядом історичної справедливості у сучасних умовах.

Під «русским миром», як вбачається з того ж таки контексту книги-альбому, слід розуміти розгалужену ідеологічну систему, побудовану на пропаганді розвитку російської культури для забезпечення відповідних

потреб закордонних росіян та спрямовану на охоплення всіх сфер життя тієї країни, у якій вона запроваджується. Така концепція вироблена в контексті загальної політики РФ щодо захисту співвітчизників закордоном, проголошеної ще після розпаду СРСР у 1991 р. та відображеної в однойменному законі від 1997 р. [2, с. 236]. Цей закон по суті надав Кремлю широкий спектр можливостей впливу на політику інших держав, тим самим не заперечуючи і поступового встановлення тотального контролю над ними. Попри досягнуті міжнародні домовленості щодо правонаступництва, влада РФ будувала плани щодо переформатування СРСР і його відновлення під своєю егідою. Не бажаючи відступати від імперських амбіцій, урядовці розробляли плани непрямої інтервенції, у тому числі на Балканах. Саме тому політику щодо поширення в регіоні «русского мира» слід трактувати в контексті впливу на місцеве населення (у тому числі, урядові кола) задля поступового утвердження там своїх позицій. Позаяк у цій діяльності важливу роль відіграє спекуляція на історичному минулому та постійне апелювання до накопиченого царською Росією арсеналу методів формування «слов'янської єдності», ретроспективний аналіз зазначених питань набуває вкрай важливого значення задля забезпечення універсальної та регіональної міжнародної безпеки на сучасному етапі.

Таким чином, концепт «русский мир» містить у собі досить потужне ідеологічне навантаження і, базуючись на перекрученнях історичного минулого Росії та слов'янських народів, застосовується для поступового руйнування культурної ідентичності та національної самосвідомості тих народів, щодо яких РФ спрямовує свої експансіоністські наміри. Він слугує для формування сприятливого середовища діяльності російської пропаганди з метою забезпечення максимально швидкого і безперешкодного втілення російського геополітичного курсу, котрий базується на стійких історично сформованих традиціях іще Московського царства та Російської імперії.

Література

1. Русское зарубежье в Болгарии: история и современность. – София, 2009. – 315 с.

2. Задорожній О. В. Анексія Криму – міжнародний злочин : моногр. / О. В. Задорожній. – Київ : К.І.С., 2015. – 576 с.

УДК 351.86(477)
Іжутова І.В.
Національний університет оборони України
ім. Івана Черняховського

ЗАСТОСУВАННЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ПІД ЧАС ВВЕДЕННЯ ВОЄННОГО СТАНУ В УКРАЇНІ

У зв'язку із актом відкритої збройної агресії Російської Федерації, що відбувся 25 листопада 2018 року в районі Керченської протоки проти групи кораблів Військово-Морських Сил Збройних Сил України, Президент України Петро Порошенко підписав Указ про введення воєнного стану в десяти областях: Вінницька, Луганська, Донецька, Запорізька, Миколаївська, Одеська, Сумська, Харківська, Чернігівська, Херсонська, а також внутрішніх водах Азово-Керченської акваторії строком на 30 діб з 26 листопада [1].

Запровадження правового режиму воєнного стану активізувало використання технологій стратегічних комунікацій як на рівні держави, так і за її межами. Посилила інформаційну війну й країна-агресор.

В Доктрині інформаційної безпеки України, затвердженої Указом Президента України, стратегічні комунікації визначені як скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави. Відповідно до вимог цього документу, Міністерство оборони України має забезпечувати функціонування системи військово-цивільних зв'язків у місцях постійної дислокації та розгортання підрозділів Збройних Сил України, інших військових формувань [2].

Саме в цей період на передній план вийшли основні складові стратегічних комунікацій – публічна дипломатія, зв'язки з громадськістю, кризові комунікації, військові зв'язки з громадськістю. Вже 26 листопада 2018 року відбувся спільний брифінг командувача Військово-Морських Сил Збройних Сил України адмірала Ігоря Воронченка і Міністра Міністерства закордонних справ України Павла Клімкіна щодо російської агресії в Азовському морі. У рамках проекту "Єдиний голос" свої дії координували Міністерство закордонних справ, Міністерство інформаційної політики та Міністерство оборони України.

В свою чергу, заступник Міністра інформаційної політики України Дмитро Золотухін наголосив, що "Україна вперше буде здійснювати комунікації в кризовій ситуації, яка називається воєнний стан. При цьому він зазначив, що у комунікаційних підрозділів органів влади є величезний досвід, адже вони з кризовими комунікаціями працюють від початку російської агресії на сході країни" [3].

Водночас і глава держави, і глава оборонного відомства проводять низку зустрічей з представниками іноземних держав в Україні та іноземних організацій, роз'яснюючи правові засади введення правового режиму [4-5].

Одразу ж після запровадження правого режиму воєнного стану країною стали поширюватися фейкові повідомлення:

розсилка від імені Міністерства оборони України SMS-повідомлень мешканцям прикордонних областей України про прибуття до військкоматів із залякуванням передати відомості про особу до суду;

фейковий наказ Міністра оборони України про вилучення транспортних засобів з іноземною реєстрацією;

розсилка повідомлень у месенджері Viber про записування всіх повідомлень та дзвінків з посиланням на федеральний уряд;

у соціальних мережах активно просувалася думка, що воєнний стан запроваджений назавжди;

також у засобах масової інформації з'являється інформація, що чоловіки у двох східних регіонах Польщі, які межують з Україною, отримують повідомлення від імені Польського державного центру безпеки з вимогою з'явитися до військових частин через події в Україні [6].

Все це робилося для поширення паніки, підвищення рівня занепокоєності серед населення. Як повідомляє Служба безпеки України, була створена мережа інтернет-провокаторів в Україні, які поширювали таку інформацію, включаючи сфабриковані фото, наприклад, магазинів з пустими полицями [7].

В таких умовах потрібно було миттєво реагувати, спростовувати перекручену інформацію через максимальне поширення правдивих повідомлень у засобах масової інформації та соціальних мережах, активізувати публічну дипломатію, міністерствам та відомствам працювати злагоджено. Заходи публічної дипломатії знайшли своє відлуння на світових майданчиках. Так, було скликане позачергове засідання Комісії Україна-НАТО, за результатами якого виступив Генеральний секретар Єнс Столтенберг та виразив повну підтримку української сторони з боку держав-членів НАТО [8].

Отже, незважаючи на початок розбудови спроможності стратегічних комунікацій, зокрема в секторі безпеки і оборони, в умовах кризи, комунікації спрацювали та досягли своєї головної мети – гарантування реалізації національних інтересів. Державні органи оперативно відреагували на кризову ситуацію, провівши інтегровану оцінку інформаційних загроз. Вищезазначене свідчить про підвищення рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам в інформаційній сфері, зі збереженням довіри до сектору безпеки і оборони України.

Література

1. Указ Президента України №393/2018 Про введення воєнного стану в Україні. Режим доступу – [Електронний доступ] https://www.president.gov.ua/documents/3932018-25594.

2. Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України". Режим доступу – [Електронний доступ] https://www.president.gov.ua/documents/472017-21374.

3. У рамках #Єдиного голосу обговорено кризові комунікації в умовах воєнного стану. Режим доступу – [Електронний доступ] https://www.kmu.gov.ua/ua/news/u-ramkah-yedinogogolosu-obgovoreno-krizovi-komunikaciyi-v-umovah-voyennogo-stanu.

4. Міністр оборони України провів зустріч з Послом Сполучених Штатів Америки в Україні. Режим доступу – [Електронний доступ] http://www.mil.gov.ua/news/2018/11/27/ministr-oboroni-ukraini-proviv-zustrich-z-poslom-spoluchenih-shtativ-ameriki-v-ukraini/?fbclid=IwAR0FHWNzMLkvZ_8-Bank8RjAUVoL_ztjtCJEPHiWqRTCoOsRUDMweBpZpVA.

5. Президент закликав світ до єдності та солідарності з Україною – інтерв'ю телеканалу CNN. Режим доступу – [Електронний доступ] https://www.president.gov.ua/news/prezident-zaklikav-svit-do-yednosti-ta-solidarnosti-z-ukrayi-51438.

6. Польським чоловікам почали масово приходити фейкові СМС про мобілізацію в країні. URL: https://tsn.ua/svit/polskim-cholovikam-pochali-masovo-prihoditi-feykovi-sms-pro-mobilizaciyu-krayini-1257015.html.

7. СБУ викрила мережу Інтернет-провокаторів, найнятих спецслужбами РФ для поширення паніки в країні після введення воєнного стану (відео). URL: https://ssu.gov.ua/ua/news/1/category/21/view/5490#.8zOjTuUt.dpbs.

8. Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the NATO-Ukraine Commission. URL: https://www.nato.int/cps/en/natohq/opinions_160789.htm.

УДК 35:172.4

Каращук А.Я.
кандидат філологічних наук,
Київський національний університет
ім. Тараса Шевченка

ІНФОРМАЦІЯ, ІНФОРМАЦІЙНІ ПРОДУКТИ, ДИСКУРС

Сьогодні дуже часто користуються термінами: «інформаційна війна», «інформаційна безпека», «інформаційна агресія». Вочевидь, що люди які використовують ці поняття та подібні не розуміють до кінця поняття «інформація».

Згідно до закону України про інформацію: інформація - це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, а захист інформації - це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї (https://zakon.rada.gov.ua/laws/main/2657-12).

Ці визначення не дають можливості вчасно реагувати на агресію на інформаційному рівні, забезпечувати інформаційну безпеку. На рівні обробки інформації мова може йти про рівень інформативності інформаційних продуктів, які людина отримує з різних джерел. Тобто на сучасному рівні інформаційних потоків мова йде про інформаційні продукти, що містять в собі не більше 1% інформації, решта - це конотаційне подання, яке встановлюється у відповідності до політики висвітлення подій автором та/або власником та/або інваріантним завданням висвітлення згідно до національних інтересів країни.

Автор розглядає поняття інформації як відповідне відображення дійсності в реальності кожного користувача інформацією [1]. Тобто, реальність як спосіб розуміння дійсності залежить від багатьох факторів. Класичним прикладом може слугувати дальтонік, який у своїй реальності сприймає відтінки зеленого кольору як червоні. В дійсності, зелене листя не змінює свої фізичні властивості, але в реальності дальтоніка стає червоним. Цей приклад ґрунтується на фізичних особливостях сприйняття декількох індивідів дійсності та перетворення її сприйняття на рівні реальності у річ, яка не відповідає дійсності. У сучасному інформаційному просторі реальність створюється в індивідуальних та масових об’єктах за допомогою дискурсивних засобів впливу інструментами художньої виразності. Так, денотат підвищення цін на комунальні послуги, в залежності від політики подання, може бути переданий в реальності як «черговий злочин злочинної влади», або як «черговий крок до здобуття незалежності». При цьому денотат знаходиться в дійсності, а в реальності змальовується необхідна конотація. На додаток до цього, реальність, яка створюється за допомогою мас-медіа, може бути у повному відриві від дійсності. Тоді ми виходимо на рівень гіперреальності згідно до Ж. Бодріяра [3].

Зв’язуючою ланкою між дійсністю та реальністю є дискурс у розумінні Йоргансена [2], а саме - система вузлових точок з тимчасовим закріпленням необхідної конотації. Це дозволяє нам сказати, що на сьогоднішньому рівні інформаційних війн не існує, а є боротьба за тимчасове закріплення вузлових точок, тобто, відбуваються дискурсивні війни. Вузлові точки, як правило, встановлюються емпірично і відповідають реперним точкам формування особистості, що дозволяє як, з одного боку, контролювати конотаційне забарвлення вузлових точок внутрішнього дискурсу, так і з іншого - планувати деконструкцію вузлових точок дискурсу опонентів. Вузлові точки мають за аналогію опорні пункти фронту, які між собою пов’язані елементами (дійсна конотація) і моментами (можлива конотація). Внутрішній дискурс, як і дискурс опонента, може бути представле-

ний як мережа опорних пунктів ліній фронту з заданими відстанями між ними, або у вигляді рибальської сіті із заданою величиною вічок у відповідності до того, яку рибу нам треба упіймати. Система вузлових точок внутрішнього дискурсу встановлюється у відповідності до головних понять формування особистості. Підтримка необхідних конотацій вузлових точок контролюється за допомогою соціологічних інструментів. Будь-яка зміна конотації вузлової точки свідчить про зовнішнє втручання та/або зовнішню агресію. Вузлові точки внутрішнього дискурсу опонентів встановлюються емпірично шляхом дослідження внутрішньо-політичного дискурсу та завдань щодо формування особистості на рівні школи та вишів. Після встановлення вузлових точок, ставиться завдання із зміни конотації у сприйнятті вузлової точки, для чого опрацьовується, у відповідності до бюджету і наявного часу, медійний план дій. Тобто, на рівні забезпечення національної безпеки в інформаційному просторі, за умови відкритості інтернет-простору, інструмент дискурсивної безпеки стає чи не єдиним дійовим інструментом убезпечення національних інтересів.

Література

1. Щедровицкий Г.П. Лекции по психологии // Вопросы саморазвития человека. – Вып. 3. – К., 1991.

2. Marianne W Jørgensen, Louise J Phillips Discourse Analysis as Theory and Method SAGE, 2002-229 ISBN 0761971122, 9780761971122

3. Бодрийяр Ж. Симулякры и симуляция / Жан Бодрийяр ; [пер. с фр.О. А. Печенкина]. – Тула : Тульский полиграфист, 2013. – 204 с.

УДК 351

Коваленко Є.В.
кандидат юридичних наук,
Інститут підготовки юридичних кадрів для СБ України
Національного юридичного університету
імені Ярослава Мудрого
Плетньов О.В.
кандидат юридичних наук,
Інститут підготовки юридичних кадрів для СБ України
Національного юридичного університету
імені Ярослава Мудрого

ПЕРЕДУМОВИ ЗАГРОЗ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПЕРСПЕКТИВИ ЇХ ПОДОЛАННЯ

Автори електронного довідника з інформаційної безпеки ще у 2004 році підкреслювали, що інформаційний вплив на державу, суспільст-

во, громадянина зараз більш ефективний і економний, ніж політичний, економічний і навіть воєнний. Країни з більш розвиненою інфраструктурою, встановлюючи технологічні стандарти й надаючи покупцям свої ресурси, визначають умови формування і діяльності інформаційних структур в інших країнах, здійснюють суттєвий вплив на розвиток їхніх інформаційних сфер [1, с. 3].

12 років по тому в умовах воєнного конфлікту з Російською Федерацією законодавцем у Стратегії кібербезпеки України, затвердженій Указом Президента України від 15 березня 2016 року № 96/2016, наголошено на тому, що кіберпростір поступово перетворюється на окрему, поряд із традиційними «Земля», «Повітря», «Море» та «Космос», сферу ведення бойових дій, у якій все більш активно діють відповідні підрозділи збройних сил провідних держав світу. З урахуванням широкого застосування сучасних інформаційних технологій у секторі безпеки і оборони, створення єдиної автоматизованої системи управління Збройних Сил України оборона нашої держави стає більш уразливою до кіберзагроз.

В сучасних умовах економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Цьому сприяє широка, подекуди домінуюча, присутність в інформаційній інфраструктурі України організацій, груп, осіб, які прямо чи опосередковано пов’язані з Російською Федерацією. І означена тенденція буде зберігатись протягом значного часу, що є однією із головних причин для активізації зусиль у напрямку зміцнення інформаційної безпеки нашої держави та її складової – кібербезпеки.

Запорукою забезпечення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, є створення національної системи кібербезпеки. Закон України «Про основні засади забезпечення кібербезпеки України» у ст. 1 визначає кібербезпеку як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Сологуб Р., аналізуючи найбільш ефективні напрямки захисту критичної інфраструктури країни у кіберпросторі, підкреслює, що «потреба в кібербезпеці з’явилася порівняно недавно, коли люди створили новий простір для життя – кіберпростір. У ньому не лише зберігається і передається інформація, а й відбуваються тисячі процесів життєдіяльності окремих людей, держав і суспільства в цілому. Спочатку з’явився Інтернет, в

якому люди обмінювалися інформацією. Зараз все активніше розвивається так званий Інтернет речей (Internet of Things), під яким розуміються підключені до мережі побутові предмети, які вже без залучення людей збирають та передають дані. А в недалекому майбутньому, за прогнозами, нас чекає Інтернет всього (Internet of Everything), в якому між собою будуть поєднані люди, речі, дані та процеси» [3].

Зрозуміло, що процеси глобалізації, які пришвидшуються з огляду на розповсюдження Всесвітньої мережі Internet, мають неконтрольований характер і не до кінця передбачувані наслідки. І сфера кіберзлочинності має дуже високий потенціал розвитку та підвищення своєї негативної ефективності. Нажаль, і тут необхідно констатувати невтішну динаміку, не тільки законодавчі зміни, спрямовані на боротьбу з кіберзлочинністю, але й власне технічні та програмні засоби такої боротьби, виявляються неефективними за застарілими, навіть до того, як вони можуть бути використані в правоохоронній діяльності. Причиною цьому є невідповідність швидкості розвитку засобів злочинної діяльності у кіберпросторі швидкості законодавчого врегулювання та впровадження тих або інших засобів протидії такій діяльності.

При цьому необхідно враховувати, що кіберпростір як такий може бути не тільки одним із чинників уразливості національної системи безпеки, але й засобом збільшення її потужності. Так, наприклад, дослідивши кіберпростір як новий вимір геополітичного суперництва, Д.В. Дубов дійшов до висновку, що «…національні інтереси та національна сила безпосередньо пов’язані з політикою держави щодо кіберпростору та її позиціюванням у цьому просторі, вмінням формулювати цілі щодо нього та використовувати його можливості заради збільшення власної могутності» [2, с. 36]. Також цей же автор характеризує кіберпростір як досить специфічний простір, «в якому держави змушені в умовах часткового суверенітету формувати свої позиції та захищати національні інтереси. Цікаво, що на рівні міжнародного права та усталених традицій розуміння поняття суверенітет, наявний, хоча й обмежений, суверенітет над телекомунікаційною інфраструктурою є досить неоднозначним. Фактично саме це і створює центральне тло глобального протиборства між державами за майбутнє кіберпростору» [2, с. 40].

Так, наприклад, досить цікаву позицію з приводу істотних загроз кібербезпеці держави зайняли аналітики, які є дотичними до створення Стратегії кібернетичної оборони Чехії (Національний центр кібероперацій). Так, названа Стратегія відповідає на ключові проблеми в цій області, які включають, в першу чергу, «нові тенденції роботи впливу», збільшення ризику з боку недержавних суб’єктів, кібертероризм, все більша кількість пристроїв, що працюють у мережі Інтернет, низький рівень комп’ютерної грамотності, відсутність обізнаності користувачів про

принципи безпеки в кіберпросторі і зростаючу залежність підрозділів державної оборони від інформаційно-комунікаційних технологій [4]. Характеризуючи у Концепції боротьби з тероризмом, затвердженій Указом Президента України від 5 березня 2019 року № 53/2019, об'єкти можливих терористичних посягань, законодавцем, поряд із іншими, виділено також інформаційний простір та його компоненти, одним із яких і є кібербезпека.

Таким чином все наведене вище дає підстави зробити висновок, що наразі інформаційна безпека держави та її складова – кібербезпека, особливо в період передвиборчої кампанії та виборів Президента України, є особливо уразливим об'єктом, безпека якого має бути забезпечена відповідними суб'єктами та засобами. При цьому необхідно враховувати, що, з огляду на проаналізовану вище динаміку розвитку інформаційного суспільства та злочинного інструментарію, який використовується зловмисниками у названій вище сфері, Служба безпеки України постійно стикається з новими викликами, вирішення яких залежить як від компетентності її співробітників, так і відповідних кроків законодавця у контексті забезпечення адекватних засобів протидії існуючим загрозам.

Відповідно до п. 3 ч. 2 ст. 3 Закону України «Про основні засади забезпечення кібербезпеки України» Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки. Проте наразі існуючі можливості зазначеного суб'єкта забезпечення кібербезпеки не в повній мірі відповідають небезпеці злочинних викликів та формам злочинної діяльності у кіберпросторі. З огляду на цей факт вбачається за необхідне:

- розширити перелік злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

- виділити об'єкти критичної інфраструктури як додатковий предмет злочинів, передбачених Особливою частиною КК України;

- передбачити звільнення від кримінальної відповідальності осіб, які за власною ініціативою здійснюють відповідальний пошук уразливостей у системі захисту об'єктів критичної інфраструктури;

- розширити перелік оперативно-розшукових та контррозвідувальних заходів, які проводяться у такій специфічній сфері як інформаційна безпека.

Вказані дії, проведені у комплексі із іншими заходами організаційно-правового характеру, сприятимуть підвищенню рівня захищеності інформаційної безпеки та стануть підґрунтям для формування нової концепції діяльності правоохоронних органів в сучасних умовах.

Література

1. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / за ред. Кривуци В.Г. – Київ: ООО «Д.В.К.», 2004. – 508 с.

2. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – С. 36.

3. Сологуб Р. - Як захистити критичну інфраструктуру країни у кіберпросторі / Р. Сологуб / Електронний ресурс. Режим доступу: https://biz.nv.ua/ukr/experts/jak-zakhistiti-najtsinnishu-informatsiju-u-kiberprostori-2510093.html.

4. У Чехії розробили стратегію кіберзахисту на п’ять років / Електронний ресурс. Режим доступу: https://ua.korrespondent.net/world/4001251-u-chekhii-rozrobyly-stratehiui-kiberzakhystu-na-piat-rokiv.

У*ДК 351*

Коваленко Л.П.
доктор юридичних наук, професор,
Національний юридичний університет
імені Ярослава Мудрого

СУЧАСНИЙ СТАН РОЗВИТКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СФЕРІ ОБОРОНИ

Становлення в розвинутих демократичних країнах громадянського суспільства є формування нової системи цінностей, в якій ключове значення має життя людини, її права і безпека. Для цивілізованого громадянського суспільства неприйнятний воєнний шлях розв’язання внутрішньополітичних, зовнішньополітичних проблем, ведення бойових дій пов’язано зі значними людськими втратами, якщо виникають загрози існування суспільства. Використовувати ж воєнну силу в ситуаціях, які не загрожують існуванню цих країн, стає все більш складніше по мірі розвитку громадянського суспільства.

Досвід воєнних конфліктів в останнє десятиріччя свідчить про те, що рівень допустимих для демократичних країн втрат становить сьогодні десятки, якщо не одиниці людських життів і це стає одним з найважливіших факторів стримування цих країн від застосування воєнної сили. Подальша, глобалізація, і, особливо, зростаючий збіг економічних і політичних інте-

ресів розвинених демократичних країн, виключають воєнні конфлікти між ними. Їхні загальні інтереси вимагають, крім усього іншого, надійного забезпечення безпеки кожної держави і можливості спільного вирішення гострих світових проблем, у тому числі з застосуванням сили. Основними засобами вирішення гострих політичних проблем стали економічна і культурна експансії, міжнародні економічні і політичні санкції, й у крайніх випадках – загроза застосування сили там, де це не загрожує серйозними людськими втратами по обидва боки. У цих умовах інформаційна зброя може стати дуже ефективним силовим засобом, що дозволяє вирішувати багато конфліктів без застосування традиційних засобів збройної боротьби.

Значущість інформаційної безпеки як складової національної безпеки України пояснюється залежністю реалізації найбільш важливих інтересів України у воєнній сфері від інформаційних загроз. З аналізу найбільш небезпечних загроз важливим національним інтересам України у воєнній сфері випливає, що реалізаційною основою більшості цих загроз є інформаційна [1; с. 27]. З-поміж інших загроз стабілізації воєннополітичної обстановки та недопущення збройних конфліктів в Центральній Європі розглядаються такі: висунення територіальних претензій до України; втручання у внутрішні справи України; нестабільність воєнно-політичної обстановки навколо України; активізація сепаратистських сил і підтримання їх ззовні; заяви та акції, що дискредитують внутрішню і зовнішню політику України; войовничість політичного керівництва сусідніх країн; загострення міжетнічних і міжконфесійних суперечностей; нестабільність соціально-політичної обстановки в суміжних з Україною країн. Не виникає сумніву в тому, що всі ці загрози тією чи іншою мірою реалізуються на інформаційному рівні, причому їх інформаційна складова досить вагома.

Крім того, за оцінками вітчизняних експертів з проблем інформаційної безпеки [2; с.61], що сформовані на основі аналізу іноземного впливу на інформаційний медіа – і кіберпростір України, існують ознаки реальних загроз для нашої держави. Про це свідчать такі основні тенденції: цілеспрямоване формування окремими іноземними державами негативного міжнародного іміджу України; здійснення рядом зарубіжних країн потужного інформаційного тиску на Україну з метою спонукання українського керівництва до прийняття вигідних для цих країн рішень у внутрішньо- та зовнішньополітичній сферах; посилення інформаційних заходів з перешкоджання реалізації Україною її зовнішньополітичного курсу та спонукання її до участі в проектах, які в сучасних умовах не вигідні нашій державі; дискредитація нашої держави як конкурента у сфері міжнародного військово-технічного співробітництва; зростання для України загроз кібернетичних атак, що обумовлено появою нових, більш досконалих зразків кібернетичної зброї. Однією з істотних загроз підтримуванню боєздатності формувань Воєнної організації є втрата престижності воєнної служби і зниження моральнопсихологічного рівня особового складу. Ця загроза має інформаційний характер. Такі загрози розвитку системи інформаційної

безпеки в сфері оборони, як відсутність фахівців, в цій царині, послаблення уваги до розвитку систем інформаційної безпеки, прогалини в інформаційному законодавстві, відставання в розробленні критичних технологій і технологій подвійного призначення та послаблення контролю за системою підготовки наукових кадрів мають суто інформаційний характер.

Слід зазначити, що йдеться не про абсолютизацію інформаційних факторів у реалізації наведених загроз, а про те, що вони, поряд з економічними, політичними, соціальними та іншими факторами, є домінуючими. Тому ефективність своєчасного виявлення та нейтралізації розглянутих загроз інформаційній безпеці у оборонній сфері істотно залежить від виваженості й активності заходів щодо забезпечення національної безпеки на інформаційному рівні. Таким чином, забезпечення інформаційної безпеки держави є проблемою високої складності та потребує комплексного підходу. На нашу думку, для ефективного функціонування системи інформаційної безпеки України сукупність зазначених організаційно-технологічних та організаційно-правових заходів слід поєднати в систему адміністрування інформаційною безпекою в межах забезпечення оборонної безпеки України. Відповідно до теоретичних розробок спеціалістів у галузі інформаційної безпеки, основними напрямами забезпечення інформаційної безпеки є правовий, організаційний, інженерно-технічний. Застосування всіх цих напрямів є необхідним для формування комплексної інформаційної безпеки держави.

Література

1. Коваленко Л.П. Теоретичні проблеми розвитку інформаційного права України: монографія /Л.П. Коваленко. – Х.: Право, 2012. – 248 с.

2. Інформаційне право **:** підручник / В. Я. Настюк (кер. авт.кол.), Л. П. Коваленко та ін.; за заг. ред. В. Я. Настюка, Л. П. Коваленко – Харків : Право, 2016. – 280 с.

УДК 342.72/.73-74

Корж І.Ф.
доктор юридичних наук,
старший науковий співробітник,
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

СПІВВІДНОШЕННЯ ПРАВА І ОБОВ'ЯЗКУ

Права людини в сучасному світі – це і здобуток людства, і одночасно проблема, вирішення якої знаходиться у центрі практичної діяльності міжнародного співтовариства і кожної держави. Права людини – це її мо-

жливість діяти певним чином для того, щоб забезпечити своє нормальне існування, розвиток і задоволення власних потреб. В інформаційній сфері – це універсальне конституційне право на інформацію, що містить у собі такі конкретні можливості, які в сукупності і становлять так звані інформаційні права. Як зазначено в ч. другій ст. 34 Конституції України, «кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір» [1]. Здійснення цих прав може бути обмежене законом.

Однак, вже зараз помітно, що абсолютизування права призводить до настання негативних наслідків – прояву «правового екстремізму», тобто зловживання правом, прояву утриманства, паразитизм тощо. Прояв «правового екстремізму» в інформаційній сфері проявляється насамперед у тому, що інформація про особу, яка часто є спотвореною і недостовірною, поширюється без відома і дозволу зазначеної особи. З огляду на зазначене, питання зловживання правом на інформацію та її поширення, яка є не просто інформаційним продуктом, а часто використовується як засіб боротьби з опонентами, в українському суспільстві набуло значної гостроти.

Якщо говорити про «зловживання правом» загалом, то мова може йти про вжиття суб'єктивного права таким чином, що внаслідок цього суспільним відносинам завдається шкода. Під зловживанням правом в наукових дослідженнях розуміється головним чином «шикана», тобто здійснення суб'єктивного права з метою нанесення шкоди другій особі. «Шикана» в даному випадку є такою формою реалізації права, за якою суб'єкт її поширення не співвідносить свою поведінку з принципами розумності і добропорядності.

З другого боку – зловживання правом можна розглядати як протиправні дії, тобто як звичайне правопорушення. Є думка дослідників, що зазначене може вважатися правомірною діяльністю, однак в даному випадку дана діяльність є аморальною. Необхідно зазначити, що в наукових дослідженнях поняття «зловживання правом» суттєво відрізняється від поняття «протиправна діяльність». До того ж випадки зловживання правом складніше розпізнати від випадків протиправної діяльності. Однак зловживання правом, в залежності від його мети, в кінці кінців може призвести до правопорушення. Водночас, якщо протиправна діяльність навіть формально не базується на праві і само по собі є протиправним в чистому виді, то зловживання правом опирається на суб'єктивне право і формально не суперечить об'єктивному праву. Таким чином, якщо у особи немає суб'єктивних прав, зловживати правом вона не зможе. Водночас, вчинити протиправне діяння за відсутності суб'єктивних прав особа може.

У розвиненому суспільстві права обов'язково кореспондують обов'язкам, і це стає найважливішою запорукою розвитку держави. Чим відрізняються дані категорії, що є первинним, а що – вторинним? Про право ми вже говорили вище. Обов'язки – це сукупність загально-

обов'язкових норм, невиконання яких тягне за собою передбачену законом відповідальність. Деякі з них закріплені формально, інші – розуміються умоглядно. Відмінність між ними полягає в імперативності: використання права на інформацію – це можливість, а дотримання обов'язку у цій сфері – необхідність; невиконання обов'язку переслідується за законом, а не використання права відповідальність не передбачає; правами наділені усі люди, а обов'язками наділено значно менше коло людей.

Конструкція єдності права і обов'язку представляє собою певну систему, елементи якої лише у своїй сукупності утворюють нову якість, яке відсутнє у них окремо. Зазначений принцип єдності має для суспільства певне значення, оскільки забезпечує баланс приватних і публічних інтересів; сприяє розвитку індивідуальної правосвідомості, формуванню ціннісно-правових орієнтацій; є запорукою еволюційного, гармонійного розвитку особистості і суспільства тощо.

Необхідно зазначити, що специфіка конституцій європейських демократичних країн полягає в чіткому відображенні в конституційному тексті принципу єдності прав і обов'язків, що є своєрідним «врівноваженням» позиції особи у відносинах з представником влади.

В Україні ж, конституційно-правова дійсність полягає в тому, що баланс між правами і обов'язками в Основному законі порушено на користь прав осіб. Тому, допоки в Україні не буде оптимізовано згаданий баланс між правами і обов'язками, а сприятиме цьому грамотне, логічне, послідовне оперування правами і обов'язками; правильна розстановка стимулів і обмежень (дозволів, заборон, заохочень, покарань), послідовне закріплення в законодавстві вимог сумлінного і розумного здійснення прав і виконання обов'язків, усунення дисбалансу між правами і обов'язками в Конституції України тощо, у країні будуть мати місце факти зловживання правом на інформацію, на її поширення, що проявляється у безкарному вчиненні наклепів, охаювання тощо. Свіжим прикладом зазначеного є ситуація із так званим «антифашистом» Володимиром Скачко, фігурантом «Миротворця», антиукраїнським пропагандистом, учасником російської інформаційної спецоперації проти України, маніпулятором публічно значимою інформацією, який заперечує російську агресію [2].

Література

1. Конституція України від 28 березня 1996 року // Відомості Верховної України. – 1996. –№ 30. – Ст. 141.

2. СБУ провела обыск у автора ресурса "Антифашист" Скачко [Електронний ресурс] URL : https://gordonua.com/news/politics/sbu-provela-obysk-u-avtora-resursa-antifashist-skachko-788275.html (дата звернення 08.03.19).

УДК 351.746.1 (477)
Кравченко Р.М.
кандидат юридичних наук,
Служба безпеки України

ЩОДО ДІЯЛЬНОСТІ ОРГАНІВ ВІЙСЬКОВОЇ КОНТРРОЗВІДКИ СБ УКРАЇНИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Служба безпеки України визначена законодавцем як державний орган спеціального призначення з правовими функціями, який забезпечує державну безпеку, тобто є одним із суб'єктів забезпечення державної безпеки України, а відтак – одним із провідних суб'єктів реалізації державної політики в інформаційній сфері [1-3].

Згідно із Законом України «Про Службу безпеки України», органи військової контррозвідки створюються для контррозвідувального забезпечення Збройних Сил України (ЗСУ) і Державної прикордонної служби України та інших військових формувань, дислокованих на території України [1].Однією з важливих складових контррозвідувального забезпечення Збройних Сил України є реалізація заходів в інтересах забезпечення інформаційної безпеки ЗСУ.

У Збройних Силах України існує система забезпечення кібербезпеки, до функційякої належить контроль (моніторинг) стану кібербезпеки; проведення операції (дій) у кіберпросторі; розробка спеціальних програмних засобів; здійснення захисту інформаційно-телекомунікаційних систем від кібератак; контроль безпеки інформації в інформаційно-телекомунікаційних системах; створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах; антивірусний захист в інформаційно-телекомунікаційних системах.

Генеральний штаб Збройних Сил України організовує заходи із кібернетичного захисту в сфері оборони і контролює їх виконання, координує роботу зі створення та захисту єдиної автоматизованої системи управління Збройними Силами України, впроваджує сучасні інформаційні технології в діяльність органів воєнного управління, здійснює стратегічне планування використання Збройних Сил у кібернетичній війні [4].

Основними об'єктами інформаційних загроз та застосування інформаційної зброї проти Збройних Сил України як у мирний, так і у воєнний час є людські ресурси та інформаційна інфраструктура ЗСУ, котра вирішує завдання управління військами і бойовими засобами збору та обробки інформації[5].Так, інформаційними загрозами функціонуванню Збройних Сил України є наступні:

- поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди Міністерству оборони України та Збройним Силам України;

- кібератаки та прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожують сталому та безпечному функціонуванню інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем Міністерства оборони України та Збройних Сил України;

- зовнішні негативні інформаційні впливи на свідомість особового складу Збройних Сил України через засоби масової інформації, а також мережу Інтернет;

- порушення встановленого регламенту збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління військових частинах та установах Міністерства оборони України та Збройних Сил України;

- несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони;

- перехоплення інформації в телекомунікаційних мережах, радіоелектронне придушення засобів зв'язку та управління;

- недостатній рівень розвитку інформаційної інфраструктури Міністерства оборони України та Збройних Сил України, низький рівень інформатизації органів військового управління, що унеможливлює здійснення оперативного контролю, завчасного прогнозування, виявлення та реагування;

- неконтрольована експансія іноземних сучасних інформаційних технологій, відставання вітчизняних наукоємних і високотехнологічних виробництв у сфері телекомунікаційних засобів та інформаційних технологій;

- використання неліцензованого і несертифікованого програмного забезпечення, засобів і комплексів обробки інформації в інформаційних та інформаційно-телекомунікаційних системах Збройних Сил України[5].

Побудова ефективної системи контррозвідувальних, пошукових, режимних та адміністративно-правових заходів органів військової контррозвідки СБУ потребує врахування зазначених інформаційних загроз функціонуванню Збройних Сил України і реалізації на цій основі адекватної протидії з використанням специфічних форм і методів в інтересах забезпечення інформаційної безпеки ЗС України.

Література

1. Закон України "Про Службу безпекиУкраїни" – [Електронний ресурс]. – Режим доступу:https://zakon.rada.gov.ua/laws/show/2229-12.

2. Закон України «Про національну безпеку України». [Електронний ресурс]. – Режим доступу: https: //zakon.rada.gov.ua/laws/show/2469-19.

3. Інформаційна безпека держави / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.]; в 2 т. – Т.1 / за заг. ред. В.В. Остроухова – К.: ДНУ «Книжкова палата України», 2016. – 264 с. – С. 237.

4. Формирование организационно-правовой системы защиты национальной инфраструктуры от киберугроз / [Бик В.В., Климчук А.А., Панченко В.Н., Петров В.В.]. – К.: Академпресс, 2013. – 220 с.– С. 22.

5. Проблеми інформаційної безпеки держави у воєнній сфері, шляхи їх вирішення: матеріали науково-практичного семінару. – Київ: НУОУ, 2015.– 52 с. – С. 24.

6. Підхід до класифікації кібернетичних загроз. –/ Ю.Г. Даник, В.І. Шестаков, С.В. Чернишук // Збірник наукових праць Національної академії Державної прикордонної служби України. Сер. : Військові та технічні науки. – 2014. – № 1. – С. 314-329. – [Електронний ресурс]– Режим доступу: http://nbuv.gov.ua/UJRN/soi_2013_9_32.

УДК 341.824

Кульчицький В.В.
Служба безпеки України

СОЦІАЛЬНІ МЕРЕЖІ ТА ІНФОРМАЦІЙНА КУЛЬТУРА ЯК ЧИННИКИ ВПЛИВУ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ

Питання вивчення специфіки формування та використання ресурсів соціальних медіа актуалізується з огляду на те, що в умовах інформаційного суспільства домінуючі функції і процеси дедалі більше виявляються організованими за принципом мереж.

У наш час соціальні мережі асоціюються з особливим видом комунікацій, які є основою для створення і підтримки особистих та професійних зв'язків між людьми. Як справедливо зазначає Г. Бакулєв, «нові медіа часто дають людям те, що вони хочуть, навіть якщо довгоочікувані наслідки можуть виявитися негативними. На відміну від звичних медіа, вони не мають зв'язків з іншими традиційними соціальними інститутами, які відчувають відповідальність перед суспільством. Адаптація до нових медіа та їхньої специфіки часто підриває існуючі соціальні зв'язки. Мінлива медіа індустрія змушує мінятися й інші суспільні інститути, включаючи політичні, релігійні, ділові, військові й освітні» [1].

Соціальні мережі дедалі глибше входять у життя суспільства, спричиняючи в ньому соціокультурні зрушення. Водночас і суспільні процеси значною мірою проектуються на соціальні медіа. Структура, контент соціальних мереж, тематика спілкування користувачів відображають актуальні проблеми суспільного життя. Насамперед мова йде про творчу самореалізацію особистості, її самовираження через спілкування, налагоджування професійних та особистісних зв'язків, розвиток соціальної журналістики.

Сьогоднішній етап розвитку цивілізації характеризується становленням глобального інформаційного суспільства, в якому основним стратегічним ресурсом є інформація. Нові інформаційно-комунікаційні технології

все більш широко проникають практично у всі сфери життєдіяльності суспільства, змінюючи умови праці і побуту людини, формуючи у нього нові потреби, стереотипи поведінки, а також нові уявлення про якість життя, простір і час.

Інформатизація соціального простору, прискорення процесів передачі і обробки інформації, розвиток мережі Інтернет та соціальних медіа стали передумовами формування нової якості відносин особи і соціуму, становлення нового типу культури, якій дають різноманітні назви: Інтернет-культура, електронна, комп'ютерна, ІТ-субкультура, нова інформаційна культура, кіберкультура і т. ін.

З огляду на такі властивості, як доступність, анонімність, оперативність, високий рівень довіри, сегментацію за інтересами, соціальні сервіси є гнучким та зручним інструментом прихованого інформаційного впливу – маніпулювання суспільною або масовою свідомістю [2].

Зважаючи на викладене, варто зауважити, що новітні технології та комунікації здатні вдосконалити методи забезпечення інформаційної безпеки, але окрім цього і можуть створювати серйозні загрози. Тенденції негативного впливу соціальних мереж на забезпечення інформаційної безпеки залишаються недостатньо усвідомленими сучасним суспільством.

В основі розвитку соціальних мереж лежать такі чинники, як інформаційні потреби людини, її потреби в самоактуалізації та самореалізації і водночас відповідний рівень розвитку інформаційних технологій, що створює необхідні умови для задоволення цих потреб. Разом з цим, інформатизація соціального простору, прискорення процесів передачі і обробки інформації, розвиток мережі Інтернет та соціальних медіа стали передумовами формування нової якості відносин та становлення нового типу інформаційної культури, яку необхідно розглядати як обов'язкову умову забезпечення інформаційної безпеки.

Вплив інформаційних процесів на всі сфери життєдіяльності суспільства актуалізував найважливіші питання соціального буття, у тому числі питання інформаційних загроз, що спричинило пильну увагу до інформаційної безпеки. Щоб забезпечити інформаційні, потреби інформація повинна відповідати певним вимогам. По-перше, інформація має бути відносно повною. Повнота інформації характеризується її достатністю для прийняття правильних рішень. По-друге, інформація має бути достовірною, бо спотворена інформація приводить до прийняття неправильних рішень. По-третє, інформація має бути своєчасною, оскільки необхідні рішення ефективні лише тоді, коли вони приймаються вчасно.

Враховуючи ці три складові, можна сформулювати наступне визначення: інформаційна безпека – стан інформаційного середовища, що забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації і захист суб'єктів від негативної інформаційної дії.

Інформаційна безпека тісно пов'язана з інформаційною культурою, під якою розуміється здатність ефективно використовувати його інформа-

ційні ресурси і засоби інформаційних комунікацій, а також застосовувати для цих цілей передові досягнення в області розвитку засобів інформатизації і інформаційних технологій [3].

Під інформаційною культурою особистості розуміється властивість особистості, що характеризує її як суб'єкта інформаційної діяльності і визначає відношення до функціонування і розвитку інформаційної сфери суспільства [4].

Таким чином, інформаційна культура є одним з головних чинників забезпечення інформаційної безпеки і у свою чергу безпосередньо від неї залежить. Вона всесторонньо впливає на інформаційну безпеку: у вигляді культури інформаційно-професійної компетенції (безпека інформації) тв у вигляді культури інформаційної безпеки (інформаційно-психологічна безпека). Культура ж інформаційного самозахисту, що комплексно формується культурою інформаційно-професійної компетенції і культурою інформаційної безпеки, визначає уміння особистості поводитися з інформацією без нанесення шкоди собі та іншим учасникам інформаційних відносин; здатність протистояти інформаційним загрозам і зберігати психічне здоров'я в умовах негативного інформаційного впливу.

Література

1. Бакулев Г.П. Массовая коммуникация : западные теории и концепции. – М. : Аспект Пресс, 2005. – 176 с.

2. Панченко В.М., Полевий В.І. Методика виявлення ознак інформаційного впливу в засобах масової інформації // Інформаційна безпека людини, суспільства, держави. – 2011. – № 3(7). – С. 67-73.

3. Колин К.К. Социальная информатика : учебное пособие для вузов / К.К. Колин.– М. : Фонд "Мир", 2003. – 432 с.

4. Алиева М.Ф. Информационная безопасность как элемент информационной культуры // Вестник Адыгейского государственного университета. – 2012. – № 4(108). – Режим доступа : http://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-element-informatsionnoy-kultury.

УДК 004.056.5

Кухарська Н.П.
кандидат фізико-математичних наук, доцент,
Львівський державний університет безпеки життєдіяльності

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ЕЛЕМЕНТ КОРПОРАТИВНОЇ КУЛЬТУРИ

Чотири з п'яти компаній недооцінюють ризики інформаційної безпеки (ІБ), пов'язані з людським фактором. Результати опитувань свідчать [1]:

• 69 % респондентів ніколи не навчались основам кібербезпеки у своїх компаніях.

• 15 % учасників опитувань повідомили, що їхні роботодавці обмежилися мінімальним обсягом інформації щодо ІБ. Навчання не виходило за рамки ”у випадку неполадок перевантажте комп’ютер”; правила кібербезпеки не розглядалися.

• 16 % респондентів мали якісні тренінги з детальними розповідями про ІБ та актуальні загрози.

• 70 % учасників повідомили, що недостатньо знайомі з темою безпеки бездротових мереж, зокрема загрозами для Wi-Fi.

• 63 % респондентів вважають, що їм бракує знань для захисту від шифраторів (програм-вимагачів).

• 57 % учасників опитувань хотіли би знати більше про безпеку паролів.

• 51 % про захист від “класичних” інструментів інтернет-шахраїв – фішингу та спаму.

Для абсолютної більшості працівників компаній інформаційна безпека не належить до основного виду діяльності і не є пріоритетом № 1. Керівники організацій, в яких донедавна переважали ”аналогові”, а не digital-підходи до ведення бізнесу, як правило, не приділяють належної уваги формуванню культури інформаційної безпеки. Звідси і наслідки: працівники не вміють розпізнавати весь спектр хитрощів, яким користуються зловмисники. Вони не вміють виявляти фішингові розсилки, шкідливі домени, небезпечні вкладення в e-mail.

Термін культура безпеки є порівняно “молодим”. Вперше він був використаний у 1986 році Міжнародною консультативною групою з ядерної безпеки в рамках досліджень, що стосувались причин і наслідків чорнобильської аварії [2]. У 1989 році консультативна група підготувала ”Основні принципи безпеки атомних станцій” (INSAG-3). У згаданому документі поняття ”культура безпеки” почало наповнюватися змістом, були визначені цілі і принципи досягнення належного рівня безпеки. На цьому етапі культура безпеки визначається як важливий управлінський принцип, а її ключовим елементом вважається ”психологія безпеки” [3].

За тридцять років, що пройшли з того часу, термін культура безпеки не тільки не втратив своєї актуальності, а став активніше розвиватися. Культура безпеки як елемент корпоративної культури вийшла за межі атомної галузі і впроваджується сьогодні компаніями у різних сферах.

На даний момент немає єдиного визначення культур и безпеки і немає загальноприйнятого способу для її оцінки. Грачов А. А. зазначає: ”Формування культури безпеки передбачає формування цінностей безпеки, норм безпечної поведінки і базових уявлень, що реалізують ці цінності і норми”[4]. Купріянова І. А., розглядаючи поняття культури безпеки, надає великого значення документальному оформленню правил й інструкцій з

безпеки. На її думку ”культура безпеки є системою норм і вимог, належне дотримання яких гарантуватиме якість професійної діяльності” [2].

Reason J. виділяє п’ять компонентів культури безпеки: культуру інформованості (informed culture) – збір даних про помилки і порушення; культуру звітності (reporting culture) – працівники відкрито і чесно повідомляють про помилки і порушення і беруть участь в управлінні безпекою в організації; просто культуру (just culture) – висока відповідальність кожного працівника за безпеку; культуру гнучкості (flexible culture) – неформальне, гнучке ставлення до реалізації змін у разі їх необхідності і культуру навчання (learning culture) – використання результатів аналізу порушень і помилок для цілеспрямованого навчання персоналу [5]. Перелічені компоненти відображають основні особливості культури безпеки.

Культура інформаційної безпеки передбачає дотримання усіма працівниками організації елементарних правил “цифрової гігієни”:

- регулярно оновлювати ПЗ і антивіруси;
- не відкривати незрозумілі вкладення;
- не переходити за посиланнями в листах від невідомих адресатів;
- не користуватися сайтами з сумнівною репутацією;
- застосовувати різні ноутбуки (планшети) для роботи і розважального серфінгу в Інтернеті;
- не вставляти в ПК неперевірені зовнішні носії інформації та інше.

Перелічити тут всі правила неможливо, їх є доволі велика кількість. Недосвідчені у сфері інформаційної безпеки працівники у разі будь-яких сумнівів повинні звертатися до фахівців департаментів, відповідальних за ІБ, а ті у свою чергу мають бути максимально відкриті для взаємодії з колегами з інших підрозділів при виникненні питань і проблемних ситуацій.

З метою формування культури ІБ організаціям слід регулярно проводити тренінги і семінари для підвищення обізнаності працівників. Нині набувають популярності методи навчання інформаційної безпеки, що передбачають нестандартну подачу матеріалу: плакати, заставки на робочих столах комп’ютерів з правилами ІБ, інтерактивне навчання, ігри. Можна проводити змагання з ІБ-грамотності і заохочувати кращих. Можна запустити онлайн корпоративний ресурс, на якому у форматі Q&A (Questions & Answers – питань і відповідей) максимально доступною мовою будуть описані найбільш поширені види комп’ютерних загроз, способи їх розпізнавання і нейтралізації. Також при першій-ліпшій нагоді бажано пояснювати, навіщо те чи інше правило ІБ придумане, що воно дає компанії і які імовірні збитки, якщо його не виконувати.

Керівництво має подавати приклад своїм підлеглим, як вести себе в тій чи іншій ситуації, позаяк політика подвійних стандартів (говорю одне, а роблю інше) намагання впровадити культуру ІБ приведе до краху.

Як показує досвід, мати хороші регламенти ІБ недостатньо, важливо

контролювати їх виконання, забезпечувати зворотний зв'язок з працівниками, додатково навчати нетямущих і карати злісних порушників. Люди по-різному ставляться до правил: одним досить їх повідомити, іншим – раціоналізувати, пояснити, що правила корисні, третім – пригрозити покаранням. Дуже важливо реалізувати принцип невідворотності покарання – слід реагувати на кожне порушення ІБ. Якщо використовувати принцип "вибіркового правосуддя" і карати порушників вибірково, то замість поведінкового патерну "не робити" можна виховати зовсім інший патерн "робити, але не попадатись". Погано впроваджувані заборони породжують бажання їх обійти, призводять до появи у частини користувачів особливого зухвальства у порушеннях.

Процес впровадження правил ІБ у корпоративну культуру непростий і багатоплановий. Для того щоб дотримання "інформаційної гігієни" стало для працівників не просто обов'язком, а й потребою, необхідно зробити її правила зручними для виконання, інтегрувати їх в існуючі робочі процеси, не забуваючи при цьому заохочувати найбільш грамотних в плані ІБ і карати порушників.

Література

1. Семенихин И. В. Информационная безопасность необходимая составная часть корпоративной культуры компании. Как интересно и эффективно организовать обучение персонала основам ИБ. URL: https://www.youtube.com/watch?v=I6kZFNeUno8 (дата звернення: 06.03.2018).

2. Куприянова И. А. Культура безопасности ядерных объектов. Критерии оценки и способы её оценки. Ядерный контроль. – 2004. – Т. 10. – № 2. – С. 45-56.

3. МАГАТЭ. Основные принципы безопасности атомных электростанций. Серия изданий по безопасности № 75-INSAG. – 1989.

4. Грачев А. А. Организационный подход к формированию культуры безопасности работника. Знание. Понимание. Умение. – 2014. – № 1. – С. 276-287.

5. Reason J. T. Managing the risks of organizational accidents. London : Ashgate. – 1997. – 252 p.

Ландіна А.В.
кандидат юридичних наук,
старший науковий співробітник
Інститут держави і права
ім. В.М. Корецького НАН України

ОКРЕМІ АСПЕКТИ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека є важливою складовою національної безпеки і являє собою самостійну сферу забезпечення національної безпеки. В той

же час інформаційна безпека і забезпечення її правовими (доктринальними) засобами є гарантією забезпечення права людини на інформацію, на доступ до достовірної, повної та необхідної інформації тощо.

Постійно набувають все більшого значення методи управління із використанням інформаційних технологій соціальними та економічними процесами, фінансовими і товарними потоками, аналізу і прогнозування розвитку внутрішнього і зовнішнього ринків. Використання інформаційних технологій також визначає структуру і якість озброєнь, необхідний рівень їх достатності, ефективність дій збройних сил. Спроможність ідентифікувати науково-технічні та екологічні проблеми, здійснювати моніторинг їх розвитку і прогнозування наслідків безпосередньо залежать від ефективності використовуваної інформаційної структури [1].

У сучасних умовах інформаційна безпека є важливою змістовною складовою загальної національної безпеки, оскільки все більшої суспільної небезпечності набувають так звані інформаційні (гібридні) війни. В умовах стрімкого розвитку інформаційно-комунікаційних технологій, розбудови правової держави, ускладнених глобалізаційних та інтеграційних процесів, однією з нагальних проблем для України є необхідність прискорення формування комплексної системи правового регулювання сфери забезпечення інформаційної безпеки [2, с. 59]. Найбільше навантаження у цьому напрямі щодо вироблення найбільш ефективних та дієвих заходів забезпечення інформаційної безпеки в Україні приходиться саме на сферу кримінально-правового регулювання.

У сучасному суспільстві значення інформації постійно зростає – можна навіть сказати, що інформація перетворюється на найцінніший товар і продукт. С.В. Савченко зазначає: «В інформаційному суспільстві інформаційний вплив на державу, суспільство, громадян є ефективнішим, ніж політичний, економічний, військовий. Значення інформації зростає в міру зникнення національних кордонів між державами, подолання наслідків інформаційної ізоляції пострадянського суспільства (хоча ці наслідки у багатьох сферах, зокрема науковій, не подолані і дотепер)» [3].

У цих умовах і виникають ряд проблем, пов’язаних із обігом інформації. До таких можна віднести інформаційну перенасиченість суспільства; величезна кількість недостовірної та шкідливої інформації; обіг забороненої інформації, що загрожує національній безпеці держави, внаслідок інформаційного шпигунства; інформаційна агресія іноземних держав (з чим українське суспільство стикнулося останніми роками дуже тісно) та інші.

Перед органами кримінальної юстиції України постало питання вироблення і застосування ефективних засобів боротьби із негативними явищами у сфері інформаційної безпеки як складової національної безпеки і

забезпечення захисту національного інформаційного простору від протиправних дій, наслідком яких можуть суспільно небезпечні наслідки (причому нерідко не лише для України, а й для інших держав). Одним із основних засобів кримінальної юстиції у боротьбі із є криміналізація протиправних діянь у сфері інформаційної безпеки з огляду на їх суспільну небезпечність. Видається, що цей процес іще незавершений, оскільки в умовах стрімкого розвитку інформаційного простору з'являються нові протиправні діяння, які набувають все більшої суспільної небезпечні. Наприклад, так сталося із злочинами у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: наприклад, усередині XX століття цих протиправних діянь взагалі не могло бути, оскільки комп'ютерно-інформаційні технології знаходилися у зародковому стані, як і відносини у цій сфері. А з моменту прийняття чинного Кримінального кодексу і до сьогодні розділ Особливої частини КК, який передбачає відповідальність за вказані злочину перетерпів безліч змін, оскільки ця сфера суспільних відносин знаходиться у стані постійного розвитку, а це означає, що розвиваються і негативна сторона у цій сфері – правопорушення. Такі правопорушення можуть відразу мати необхідний для криміналізації рівень суспільної небезпечності або можуть набути його з часом, і тоді законодавець належним чином повинен відреагувати на їх виникнення і розповсюдження. Це може стосуватися і інших суспільних відносин, що охороняються кримінальним законодавством, у сфері яких можуть виникнути суспільно небезпечні діяння, що посягатимуть на інформаційну безпеку України.

Кримінальне законодавство України містить більше п'ятдесяти норм, у яких кримінальна відповідальність передбачена за злочини, які посягають на інформаційну безпеку (як основних, так і кваліфікованих). Серед основних складів злочинів, що посягають на інформаційну безпеку, серед особливо суспільно небезпечних можна назвати посягання на територіальну цілісність і недоторканість України шляхом публічних закликів та розповсюдження матеріалів із закликами до вчинення таких дій (ч. 1 ст. 110), державна зрада, тобто діяння вчинені на шкоду інформаційній безпеці (ч. 1 ст. 111), шпигунство (ст. 114), розголошення різноманітних відомостей, розголошення яких заборонено вітчизняним законодавством (ст. 132, ст. , ст. 159, ст. 163 та інші), надання неправдивих відомостей різного змісту (ст. 158, ст.ст. 383-387 тощо), розповсюдження шкідливої протиправної інформації (ст. 224, ст. 295, ст. 300, ст. 301), а також злочини, які посягають на безпеку людства, мир та міжнародний правопорядок, такі як пропаганда війни (ст. 436), виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436[1]), незаконне

використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала (ст. 445) та інші злочини.

Є також ряд злочинів, які також за певних умов можуть також посягати на інформаційну безпеку. До таких належать: незаконний обіг дисків для лазерних систем зчитування, матриць, обладнання та сировини для їх виробництва (ст. 203[1]), доведення банку до неплатоспроможності (ст. 218[1]), Викрадення, привласнення, вимагання документів, штампів, печаток, заволодіння ними шляхом шахрайства чи зловживання службовим становищем або їх пошкодження (ст. 357) та інші злочини.

З огляду на вказане вище, а також на досить велику кількість норм, що встановлюють відповідальність за злочини, які посягають на інформаційну безпеку як України, так можуть порушувати і інформаційні права та інтереси інших держав, можна ствердно говорити про виняткову важливість охоронюваної сфери. Навряд чи будь-яка інша сфера життя суспільства забезпечена кримінально-правовою охороною шляхом встановлення кримінальної відповідальності за ряд правопорушень краще, ніж сфера інформаційного обігу.

Але встановивши кримінальну відповідальність за злочинні посягання на інформаційну безпеку, законодавець не визначає інформаційну безпеку як один із об'єктів правової охорони у ч. 1 ст. 1 КК України. Тому вважаємо за необхідне додати у ч. 1 ст. 1 ще одну сферу суспільних відносин, які забезпечують охороною з боку кримінального законодавства, а саме – інформаційну безпеку. У зв'язку з цим пропонуємо викласти ч. 1 ст. 1 у новій редакції: «Кримінальний кодекс України має своїм завданням правове забезпечення охорони прав і свобод людини і громадянина, власності, громадського порядку та громадської безпеки, довкілля, інформаційної безпеки, конституційного устрою України від злочинних посягань, забезпечення миру і безпеки людства, а також запобігання злочинам».

Вважаємо, що таке доповнення відповідає сучасному стану розвитку і законодавства, і розвитку діяльності органів кримінальної юстиції України, а також вказуватиме на виняткове значення інформаційної безпеки як для України, так і для інших держав.

Література

1. Доктрина інформаційної безпеки України від 8 липня 2009 року (втратила чинність на підставі Указу Президента України від 6 червня 2014 року)// Електронний ресурс. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/U514_09.html.

2. Олійник О.В. Стан забезпечення інформаційної безпеки в Україні / О.В. Олійник // Юридичний вісник. – 2014. – № 2(31). – С. 59-65.

3. Савченко С.В. Лекції з інформаційної безпеки // Електронний ресурс. – Режим доступу: http://zavantag.com/docs/19/index-3282224.html.

УДК 351
Лапутніна Ю.А.
кандидат юридичних наук,
Служба безпеки України

СИСТЕМА УПРАВЛІННЯ ТОТАЛІТАРНИХ ДЕРЖАВ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Для України вважається актуальним дослідити саме систему управління тоталітарних держав в сфері інформаційної безпеки. Адже сьогодні у військово-політичному дискурсі та у практичному житті для нас не тільки існує поняття агресивна війна, але й відчуваються трагічні її наслідки. При цьому, слід зазначити, Росія, як країна агресор, розв'язала війну проти України в умовах, коли всередині цієї держави повністю згорнулися демократичні процеси. А в філософсько-ідеологічній думці запанували ідеї відновлення російської імперії на тлі пошуку спільного ворога у особі атлантизму.

Отже вся військово-політична машина РФ була спрямована на мобілізацію сил, засобів та інструментів удосконалення централізованої системи управління в безпековій сфері, формування арсеналу інструментів неконвенційного впливу на населення нашої країни з подальшим використанням збройної агресії.

Разом з цим, слід зазначити, що тоталітарні режими усвідомлюють що вони існують у світі, який в цілому не є тоталітарним. Саме тому вони вимушені створювати інструменти, якими будуть впливати на потенційні країни-мішені, які вони прагнуть повернути у сферу свого геополітичного впливу. Одним з таких інструментів є пропаганда та використання насильства. Адже, як свідчив нацистський теоретик Адамовські: «пропаганда та насильство ніколи не суперечать одне одному. Використання насильства може бути частиною пропаганди»[1].

При цьому, відмічається, що пропаганда тоталітарного режиму, як правило, спрямовується на зовні. Тож очевидним є те, що поки в РФ відбувалися зміни підходів до державного управління і згортання демократичних процесів, філософська думка розвивалася у напрямку розробки доктринального підґрунтя до ведення агресивної та експансивної політики. Так, у 2000-х роках з'являються доктрини Дугіна О., розвиваються імперські рухи. Водночас, військово-політичним керівництвом створюються передумови до розробки контентного ряду масованої пропаганди, спрямованої проти України, ведеться процес створення державно-приватної системи, здатної розгорнути агресивну інформаційну війну проти України.

Вказані дії ведуться із застосуванням методів т.зв. смислової або когнітивної війни,об'єктами впливу якої є світоглядні переконання населення та цінності, сформовані у суспільствах.

Основними каналами, які застосувала РФ проти України з використанням технології смислової війни з 2008 року, стали: телебачення (переважно серіали), кінопродукція, література. Реалізації смислової експансії сприяв: спільний інформаційний, телекомунікаційний та культурний простір пострадянського періоду.

Основними смислами, які нав'язувалися населенню України російським телеконтентом були:

«Україна та РФ – єдина країна, яка має єдиний народ, культуру, історію»;

«Більшість населення України хоче говорити російською мовою»;

«Радянська армія - основний герой Другої світової війни»;

«НАТО – агресивний ворожий блок»;

«Чорноморський флот в Криму – гарантія безпеки для України»;

«В СРСР жити було набагато краще, ніж в суверенній Україні»;

«Сучасна російська армія, спецпризначенці, правоохоронці – найбільш порядні, професійні в світі»;

«Російські спецпризначенці задушили тероризм в Чечні, тому герої».

Телепростір України майже десятиліття цілеспрямовано насичувався, головним чином, серіалами, книгами, що переформатовували ціннісно-смислові орієнтації українців.

Наступним етапом розгортання проти України інформаційного фронту з боку РФ стали російські соцмережі «ВКонтакте» и «Одноклассники», які були чітко орієнтовані на дві цільові аудиторії: ВК на молодь, ОК – на старше покоління, яке виросло в СРСР.

Враховуючи вимоги російського законодавства, згідно з якими власники соцмереж мають передавати інформацію про користувачів правоохоронним органам та спецслужбам, РФ отримала величезний масив інформації про українців, який у період перед початком військової агресії був активно застосований у маніпуляції громадською думкою в Україні.

Після відновлення суверенітету України у значній частині Донецької та Луганської областей, фактичного провалу російського бліц-кригу, інформаційну складову війни РФ проти України було вирішено посилити завдяки розвитку інтернет-ресурсів, які фактично виконують роль ЗМІ.

Вказані видання не мають відвертого антиукраїнського спрямування. Разом з цим, завдяки використанню маніпулятивних технологій стали елементом т.зв. м'якої сили. Мета подібних проектів – зміна ціннісних орієнтацій, підміна смислів цільових аудиторій в Україні в інтересах дестабілізації внутрішньо-політичної ситуації, штучного роздмухування міжетнічної, релігійної ворожнечі, провокування невдоволення населення владою, впливу на вибір українців проросійських політиків на різних рівнях, дискредитації реформ тощо.

До цих процесів спецслужби РФ активно залучають лідерів думок, блогерів, які на фоні нібито незаангажованої риторики формують громадську думку українців в інтересах країни-агресора.

Ще одним напрямком маніпуляцій з боку РФ стала цілеспрямовано робота по підриву європейського та євроатлантичного курсу України. З цією метою через різні канали інформації у цільових аудиторій в Україні здійснюється спроба формування хибних уявлень про європейські цінності. Українцям, які вийшли на Майдан відстоювати своє право розвитку країни у напрямку запровадження європейських цінностей – свободи, прав людини, демократії, верховенства права, через різні канали доводиться, що курс на Євроінтеграцію означатиме обов'язковість лібералізації потрапляння до України мігрантів, масового засилля ЛГБТ-спільнот, утиски для традиційних сімейних цінностей тощо.

Разом з цим, тоталітарні країни, маючи відповідні переваги в централізованості системи управління в сфері інформаційної безпеки, чіткий механізм підпорядкованості та контролю, відчуваючи на собі вплив міжнародного тиску з боку демократичних країн, зазвичай продовжують застосовувати пропаганду проти цивілізованого світу та країн-мішеней. Разом з цим, їм все складніше застосовувати пропаганду щодо свого населення, яке, на власні очі відчуває всі вади тоталітарного панування та висловлює сумнів щодо перспектив такого курсу країни.

Показовою при цьому, є думка російського генерала Л. Івашова, друга диктатора С. Мілошевича, про серйозні вади системи соціального управління в РФ. Російський військовий бідкається, щоправляча «еліта» не здатна виявити і визначити адекватне і природне цілепокладання для нашого суспільства, а тим більше - запропонувати обґрунтовану і ефективну методологію його досягнення. Саме з цих причин Росія , на думку військового, знаходиться поза процесом культурно-цивілізаційного творення. Більш того, з трьох матриць, що синтезують російську цивілізацію, одна, «радянська», вже майже повністю зруйнована, а дві інші: православно-слов'янська і євразійська (російсько-тюркських), - активно руйнуються.

Л. Івашов зазначає, що серед колишніх пострадянських республік Центральної Азії і Кавказу зростає розчарування поведінкою російської влади і бізнесу, Росія не запропонувала розгорнутої взаємовигідної геополітичної концепції формування майбутнього євразійського простору. Православно-слов'янський ареал також не має чіткої перспективи, крім конфлікту з Україною і трагедії Донбасу. Єдиний союзник на Балканах - Сербія рухається в бік ЄС і НАТО.

Генерал вважає, що нинішня влада РФ програла в процесі цивілізаційного будівництва все що могла. Наші надії на формування Євразійського союзу, як культурно-цивілізаційного фундаменту, розвиток ШОС, як регіонально-політичної освіти, БРІКС - як об'єднання цивілізацій не-Заходу і моделі майбутнього світоустрою, - поки не виправдовуються. Схоже, йде штучне гальмування цього процесу. Принаймні, Росія на цих напрямках втратила активність і наступальність, а культурно-

цивілізаційний будівництво заміщається спробами повсякденному економічної вигоди, причому - на китайських умовах [2].

Таким чином, не дивлячись на застосування РФ великого ресурсного, інтелектуального, військового, адміністративного потенціалу для реалізації планів відтворення імперії, в сучасному світі, який характеризується розвитком інформаційного суспільства, транскордонної комунікації, сучасних технологій обробки, зберігання, обміну інформацією, реальна ефективність досягнення кінцевої мети є досить проблемною.

Разом з цим, розуміючи тактику ведення РФ інформаційної війни, усвідомлюючи невідворотність експансивних планів країни-агресора, в сучасних умовах Україні слід зосередитися на вжитті превентивних заходів, які попереджують можливий негативний вплив смислових війн на населення.

Основна мета – інформування громадськості про зміст інформаційної агресії, форми, методологію, які використовуються РФ на шкоду інформаційній безпеці України, канали, через які здійснюються негативні впливи; сприяння розвитку «інформаційної гігієни» та медіаграмотності.

Адже усвідомлення громадянами небезпечності «інформаційної зброї» та обізнаність у сутності та формах можливого негативного впливу є однією з запорук формування стійкості нації в умовах гібридного протиборства.

Саме тому, сектор безпеки та оборони України активно працює з експертним середовищем, ІТ-сферою, громадянським суспільством, медіаспільнотою у напрямку розвитку стратегічних комунікацій, створення платформ для обговорення проблем гібридного протистояння, обміну інформацією, укріплення горизонтальних зв’язків, формування довіри та державно-приватного партнерства.

Враховуючи транснаціональний характер загроз в сфері інформаційної безпеки, одним з пріоритетів залишається розвиток міжнародного співробітництва з протидії гібридним загрозам. Одним з позитивних напрямків міжнародної співпраці вважаю створення в Службі безпеки України Ситуаційного центру протидії кіберінцидентам за підтримки Трастового фонду НАТО. Хоча з моменту його відкриття пройшло не так багато часу, можу впевнено сказати, що завдяки діяльності Центру за цей період попереджено декілька серйозних спланованих кібератак проти України.

Література

1. Hadamovsky E. PropagandaundnationaleMacht, 1933 – S. 22.

2. Гибридныевойны. Статья генерал-полковника ЛеонидаИвашова в газете «Завтра» http://www.rline.tv/podrobnosti/2018-04-03-gibridnye-voyny-statya-general-polkovnika-leonida-ivashova-v-gazete-zavtra-/ 03.04.2018.

УДК 351.1
Лашкет С.В.
Національна академія
Служби безпеки України

ІНФОРМАЦІЙНИЙ СПРОТИВ: ВЗАЄМОДІЯ МАС-МЕДІА І СПЕЦІАЛЬНИХ СЛУЖБ

Попри наявні позитивні зрушення в діяльності вітчизняних засобів масової інформації та українських спецслужб з протидії інформаційній агресії, на жаль, залишаються підстави констатувати, що брехлива провокаційна інформація російських мас-медіа досягла певної, заздалегідь спланованої, дестабілізуючої мети, оскільки керівництво Росії вибудовувало свої далекоглядні агресивні плани відносно України ще задовго до 2014 року.

Розвінчувати справжні наміри північного сусіда, убезпечувати наших громадян від негативних інформаційних впливів та протидіяти їм, покликані відповідні підрозділи Служби безпеки України та працівники українських мас-медіа всіх рівнів. Саме співробітники Служби безпеки, використовуючи доступні форми і методи контррозвідувальної та оперативно-розшукової діяльності повинні забезпечувати захист інформаційного простору України, обмежувати доступ до співвітчизників потоків спотвореної інформації. Таку ж функцію, за допомогою специфічних професійних прийомів, форм, методів та засобів, мають виконувати журналісти, редактори, ведучі теле- та радіопрограм, власники соціальних мереж в Інтернеті тощо.

Слід розуміти, що переважна більшість російських засобів масової інформації та ті, хто там працюють, перетворилися на так звані “інформаційні війська” Росії. Вкладаючи мільярди доларів на пропаганду за кордоном, Кремль серйозно розраховує повторити успіх радянської імперії, яка була другою впливовою ідеологічною силою на планеті. Проте радянська країна пропонувала світові хай утопічну, але цілісну ідеологію, набір цінностей і бажаний образ майбутнього. Сьогоднішній контент більшості російських ЗМІ скерований на розвал незалежних країн – колишніх радянських республік та їх приєднання до імперії під прикриттям реалізації плану «захисту національних інтересів росіян».

Здебільшого, наші північні сусіди використовують уже відомі та нові, спеціально вигадані, напрями інформаційної агресії. Зокрема, спроби тенденційного висвітлення історичних подій і фактів; формування думки щодо необхідності зміни конституційного ладу та євроатлантичного курсу країни; втручання у релігійні та міжконфесійні справи, заперечення і перешкоджання надання Православній церкві України Томоса; латентне ло-

біювання і фінансування «правильної» діяльності окремих проросійськи налаштованих політичних діячів, їх «просування» до найвищих щаблів державної влади і управління; розпалювання ненависті до всього українського: історії, культури, традицій, мови, державних символів тощо. Задля досягнення цієї мети застосовуються найновіші технічні засоби та всі можливі форми і методи інформаційної агресії.

Звісно, такі інформаційні втручання і спроби дестабілізації політичної ситуації в країні будуть посилюватися й наростати напередодні виборів Президента України і нового складу українського парламенту.

Водночас, в останні роки українці відчутно змінили своє ставлення до інформації пропагандистського спрямування, їх все важче увести в оману, нав'язати «потрібну» думку. Проте, слід розуміти, що тільки завдяки постійній, цілеспрямованій контрпропагандистській діяльності, спрямованій на виявлення та припинення будь-яких протиправних посягань на інформаційний простір держави та свідомість її населення, безперервній роз'яснювальній роботі ми зможемо якісно протидіяти інформаційній агресії.

Пріоритетними напрямами роботи українських спецслужб мають залишатися контррозвідувальні заходи активної протидії агресору, вони повинні спрямовувати свої зусилля на виявлення й розробку суб'єктів протиправних посягань на інформаційний простір держави, моніторинг іноземної присутності в ньому; викриття, фіксацію та документування незаконних інформаційних діянь; пошук та оприлюднення інформації компрометуючого характеру стосовно суб'єктів зовнішньої інформаційної агресії; створення інтернет-сайтів для висвітлення найбільш злободенних суспільних подій з проукраїнських позицій; добування інформації про наміри противника з метою відповідного своєчасного реагування; активне використання можливостей оперативних джерел, у тому числі джерел впливу.

Важливим у цій діяльності вбачається активна взаємодія співробітників спецслужби з представниками вітчизняних мас-медіа, побудована на правдивості й чесності, свободі та плюралізмі, недопущенні цензури, тиску і залежності. В результаті медійники матимуть надійне джерело отримання додаткової інформації для забезпечення редакційного процесу, зокрема, здобутої оперативним шляхом, підтвердити чи спростувати достовірність наявних журналістських матеріалів, а оперативні працівники – можливість доведення до широкого загалу оперативно вигідної інформації і, за потреби, встановлення необхідних конфіденційних відносин.

Загалом, незважаючи на те, що захист інформаційного простору України та убезпечення її громадян від інформаційної експансії складний, потребує часу і витрачання значних ресурсів, є всі об'єктивні підстави для впевненості у тому, що перемога буде за нами, бо, як сказав великий українець Павло Тичина, ми «єсть народ, якого Правди сила, ніким звойована, ще не була».

Література

1. Галамба М.М. Контррозвідувальний захист інформаційного простору держави від актів інформаційної експансії / М.М. Галамба // Науковий вісник НА СБ України. – 2006. – № 24. – С.162–170.

2. Лашкет С.В. Актуальні завдання контррозвідувальних підрозділів СБ України в умовах інформаційної агресії РФ // Науковий вісник НА СБ України. – 2014. – № 53. – С. 157-165.

3. Панченко В.М. Система контррозвідувальних заходів із протидії спеціальним інформаційним операціям / В.М. Панченко // Збірник наукових праць НА СБ України. – 2009. – № 31. – С.68–74.

4. Щербина Л.І., Лашкет С.В. Громадська думка як критерій оцінки ефективності діяльності Служби безпеки України // Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення : Матеріали постійно діючого науково-практичного семінару (16 травня 2014 року). – Х : Оберіг, 2014, - Вип. 5. – С. 282-289.

УДК 351

Лісовська О.Л.
кандидат економічних наук, доцент,
Національна академія Служби безпеки України

ПРІОРИТЕТИ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В УКРАЇНІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Питанням комплексного (правового, інституційного, фінансового) забезпечення інформаційної безпеки України приділялася увага з часу здобуття державної незалежності. Так, Законом України «Про інформацію» (ст. 3) забезпечення інформаційної безпеки України було віднесено до основних напрямів державної інформаційної політики [6].

Прогрес у сфері розвитку інформаційних технологій, розгортання глобального процесу інформатизації спричинили розвиток інформаційного тероризму і зростання інформаційної злочинності, що актуалізувало необхідність протидії не тільки несанкціонованому розповсюдженню, використанню і порушенню цілісності, конфіденційності та доступності інформації, але й – негативним інформаційним впливам [5].

Ситуація у сфері забезпечення інформаційної безпеки України кардинально змінилася після анексії Російською Федерацією Автономної Республіки Крим і військової агресії на Донбасі. З 2014 року протиукраїнська інформаційна активність Росії переросла у відкриту агресивну війну.

Застосування РФ технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України РФ використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігій-

ної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України [2].

Поділяючи думку Р. Марутян, що інформаційний фронт «гібридної війни» розвертається відразу на декількох напрямах (серед населення в зоні конфлікту; серед населення країни, проти якої здійснюється агресія, територія якої не охоплена конфліктом; серед громадян країни-агресора і серед міжнародної спільноти), визначаємо відповідні основні змістовні виміри дезінформації: причини й характер війни в Україні; можливість припинення війни внаслідок «незначних поступок» та вплив війни на рівень життя українського народу; історична місія Росії щодо збирання земель і захисту російськомовного населення; непричетність РФ до громадянської війни в Україні [3].

Законом України «Про національну безпеку України» визначено, що державна політика у сферах національної безпеки і оборони спрямовується на забезпечення у тому числі й інформаційної безпеки України [7].

Для посилення протидії інформаційній війні Росії проти України важливим є вивчення досвіду Європейського Союзу. Так, у Плані дій проти дезінформації, презентованому 5 грудня 2018 року у Брюсселі, визначені базові основи протидії дезінформації, а саме: покращення можливостей інституцій виявляти, аналізувати та викривати дезінформацію; посилення координації щодо спільного реагування на дезінформацію; мобілізація громадськості у протистоянні дезінформації; підвищення обізнаності та удосконалення соціальної здатності протистояти дезінформації [8].

Міністерством інформаційної політики України, яке з 2015 року є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сферах інформаційного суверенітету України, державного іномовлення та інформаційної безпеки, підготовлено аналітичну доповідь «Біла книга. Спеціальні інформаційні операції Кремля (2014-2018 рр.)». У рамках цієї доповіді зведено та проаналізовано всі основні інформаційні операції держави-агресора в інформаційному просторі України, маніпуляції, фейкові новини, факти антиукраїнської пропаганди тощо.

Зазначимо, що діяльність Міністерства інформаційної політики України профінансовано у 2018 році за рахунок видатків державного бюджету України у розмірі 857,6 млн грн (що складає 0,09 % від загальної суми видатків станом на 31.12.2018 року) [1].

Удосконалення державної інформаційної політики, спрямованої на забезпечення інформаційної безпеки України в умовах гібридної війни, передбачає, поряд із нормативно-правовим та інституційним напрямами, використання можливостей громадянського суспільства.

Конструктивна діяльність неурядових організацій була важливим чинником протидії антиукраїнській діяльності проросійських політичних партій, громадських рухів і засобів масової інформації, що фінансувалися із зовні у передвоєнний період [4]. На сучасному етапі неурядові організації беруть активну участь у реалізації державної інформаційної політики, пропагуючи переваги євроатлантичного курсу України.

Література

1. Видатки державного бюджету України (2014-2019 рр.) Функціональна класифікація, економічна класифікація, програмна класифікація. – [Електронний ресурс]. – Режим доступу :https://index.minfin.com.ua/ua/finance/budget/gov/expense/2018.

2. Доктрина інформаційної безпеки України : уведена у дію Указом Президента України : від 25.02.2017 р. № 47/2017. – [Електронний ресурс]. – Режим доступу : http:// www.president.gov.ua.

3. Марутян Р. Інформаційна складова гібридної війни проти України: сучасні виклики та загрози/ Р. Марутян. – [Електронний ресурс]. – Режим доступу : https://matrix-info.com.

4. Опалько Ю. Діяльність вітчизняних неурядових організацій, як фактор покращення ставлення до євроатлантичної інтеграції України : Аналітична записка/ Ю. Опалько. – [Електронний ресурс]. – Режим доступу : http://old.niss.gov.ua/monitor/September09/10.htm].

5. Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки ; затверджено Законом України : від 09.01.2007 р. № 537-V. – [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.

6. Про інформацію: Закон України : від 02.10.1992 р. № 2657-XII (Редакція від 01.01.2017 р., підстава – 1774-VIII).– [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.

7. Про національну безпеку України : Закон України : від 21.06.2018 № 2469-VIII. – [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.

8. Action Planagainst Disinformation – European External Action Service. – [Електронний ресурс]. – Режим доступу : https://eeas.europa.eu/.../action-plan-against-disinformation.

УДК 007.51:004.5
Лужецький В.А.
доктор технічних наук, професор,
Вінницький національний технічний університет
Дудатьєв А.В.
кандидат технічних наук, доцент,
Вінницький національний технічний університет
Миронюк В.В.
аспірант,
Вінницький національний технічний університет

БАГАТОРІВНЕВА МОДЕЛЬ УПРАВЛІННЯ КОМПЛЕКСНОЮ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

Спеціальні інформаційні операції (СІО) можуть проводитися на різних рівнях управління комплексною інформаційною безпекою: рівні окремої особи (групи осіб), одного підприємства, групи підприємств, галузі промисловості або того чи іншого регіону та нарешті держави в цілому. Відповідно до сучасної термінології СІО називають кібернетичними операціями (КО). Оскільки СІО або КО, що спрямовані на соціотехнічні системи (СТС) розраховані на ураження різнорідних складових, то доцільно їх розбити на інформаційно-психологічні операції (ІПО), що спрямовані на соціальну складову СТС, та інформаційно-кібернетичні операції (ІКО), які спрямовані безпосередньо на технічну складову СТС.

Ефективно проведені СІО, зокрема, ІПО проти так званих критичних СТС, наприклад, енергетичних об’єктів, хімічно-небезпечних об’єктів, транспортної системи можуть призвести до ризиків регіонального, державного і загальносвітового масштабів. Тому розробка багаторівневої моделі управління комплексною інформаційною безпекою є актуальною задачею.

Рішення даної загальної задачі супроводжує низка специфічних окремих задач, ефективне рішення яких можливо лише за умови реалізації системного підходу, який полягає у побудові цілісної системи комплексного захисту інформаційних ресурсів. Це пов’язано з :

– ускладненням та розширенням кола задач управління інформаційною безпекою;

– підвищенням вимог до оперативності та якості прийняття і реалізації управлінських рішень;

– високою мірою відповідальності за прийняте рішення;

– необхідністю в довгостроковому і короткостроковому прогнозуванні розвитку ситуації;

– необхідністю ефективного реагування на швидкі зміни ситуації;

– необхідністю оцінювання ризиків та загроз;

- необхідністю прийняття оптимальних і обґрунтованих рішень.

Рішення задачі розробки інтегрованої математичної моделі оцінювання рівня захищеності багаторівневої СТС буде полягати у побудові інтегрованої логіко-ймовірнісної моделі, яка об'єднує різні рівні управління комплексною інформаційною безпекою і враховує можливості проведення ІПО і ІКО [1].

Загальна математична модель оцінювання та забезпечення рівня комплексної інформаційної безпеки багаторівневої системи будується на ідеї того, що рівень захищеності держави залежить від стану захищеності підпорядкованих регіонів, рівень захищеності яких, у свою чергу, залежить від стану рівня комплексної інформаційної захищеності підпорядкованих локальних об'єктів [2]. Стан захищеності самого підприємства залежить від порушення хоча б одного з критеріїв: цілісності, доступності, конфіденційності. Кожне підприємство розглядається, як окрема загроза для відповідного регіону, який об'єднує певну кількість локальних об'єктів захисту, а кожний регіон розглядається, як окрема ймовірна загроза для держави. Такий підхід надасть можливість використання єдиної інтегрованої логіко-ймовірнісної моделі, яка формалізує всі процеси ймовірних порушень комплексної інформаційної безпеки на відповідних рівнях управління від окремого підприємства до держави. На рис. 1 представлена багаторівнева модель управління комплексною інформаційною безпекою держави.

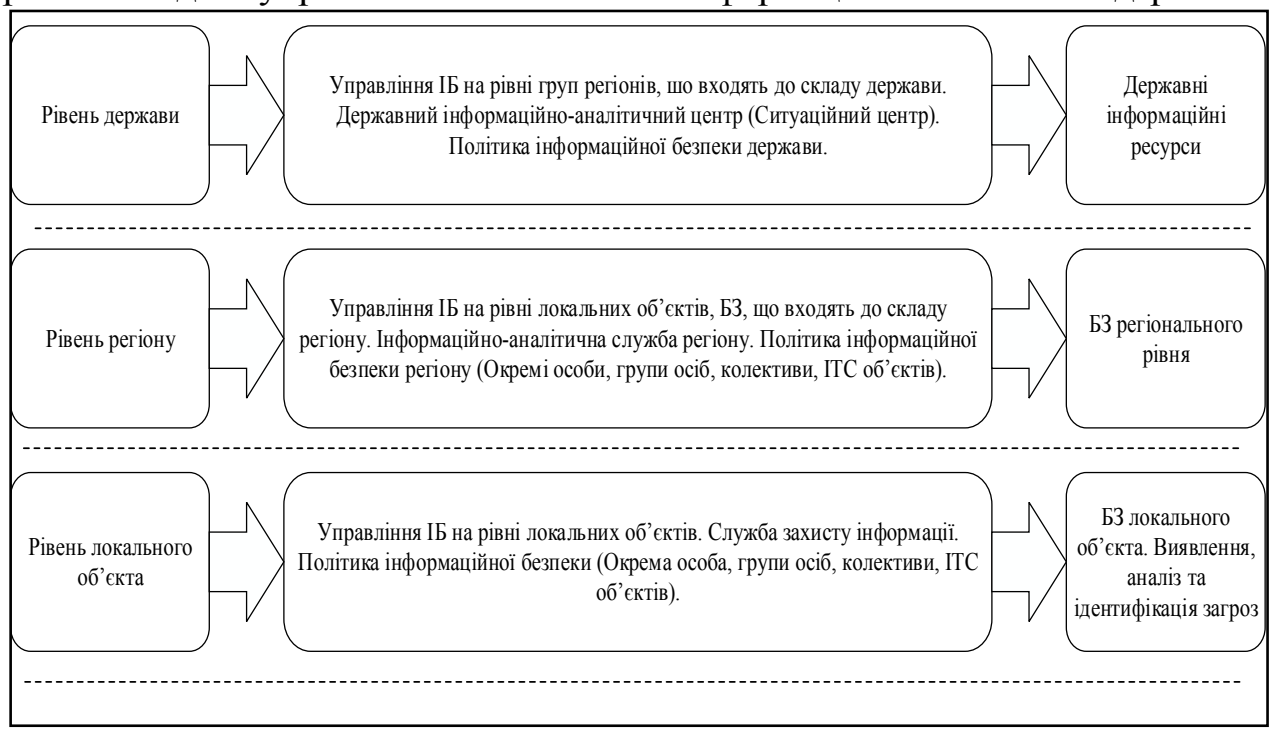


Рис. 1. Модель управління

Для оцінки адекватності запропонованої моделі потрібно проведення комп'ютерного експерименту з реальними об'єктами захисту – локальними підприємствами, групами підприємств, які складають умовний регіон

та множиною регіонів, що складають рівень держави. Для інформаційної підтримки щодо управління комплексною інформаційною безпекою розроблено програмне забезпечення, яке дозволяє автоматизувати процес аналізу рівня захищеності багаторівневої системи типу «підприємство – регіон – держава».

Література

1. Дудатьєв А. В. Розробка уніфікованих моделей системного проектування оптимальних систем захисту інформаційних ресурсів / А. В. Дудатьєв // Вісник Черкаського технологічного університету. – 2008. – № 1. – С. 3-8.

2. Дудатьєв А. В. Моделі інформаційної підтримки управління комплексною інформаційною безпекою / А. В. Дудатьєв, О. П. Войтович // Радіоелектроніка, інформатика, управління. – 2017. – № 1. – С. 107–114.

УДК 32.019.5:351.86

Манько О.В.
кандидат технічних наук,
старший науковий співробітник,
Житомирський військовий інститут ім. С. П. Корольова
Критенко О.В.
Житомирський військовий інститут ім. С. П. Корольова

АВТОМАТИЗОВАНИЙ АНАЛІЗ ТЕКСТОВИХ ПОВІДОМЛЕНЬ

В Україні вже п’ять років триває неоголошена війна з Російською Федерацією, наслідком якої є втрата частини території. Потужний деструктивний психологічний вплив із боку агресора як на силові структури України, так і на її населення, світову спільноту дозволяє державна монополія на інформаційні ресурси, що спричиняє координоване вкидання підготовленої інформації через усі федеральні канали. Тому актуальним залишається пошук нових рішень щодо протидії агресії в інформаційній сфері.

Наша держава поступово втілює механізми для протидії таким інформаційним загрозам. Вводяться обмеження доступу до матеріалів інформаційних агентств Російської Федерації з явними ознаками антиукраїнської пропаганди, публікуються спростування та інформаційні повідомлення для нейтралізації дезінформації, маніпулювання свідомістю.

За таких умов слід здійснювати дієву протидію агресії в інформаційній сфері. Одним із можливих шляхів реалізації такого завдання є автоматизація деяких етапів такого протиборства: аналізу текстових повідомлень. У доповіді пропонується підхід до автоматизації оброблення електронних текстових документів.

Наводяться результати аналізу текстів на емоційну забарвленість, яка є індикатором наявності маніпулятивної складової у тексті, з одного боку, а з іншого, – каталізатором конфліктогенів змістовної частини.

У проведеній роботі розглядається можливість визначення тональності тексту з використанням функції лексичних тональностей його складових одиниць (речень) і правил їх поєднання. Визначення самої тональності розглядається можливим на основі аналізу лексем або з використанням методу машинного навчання.

При використанні будь-якого із зазначених підходів пропонується здійснювати попереднє оброблення текстів, завданням якого є підвищення його оперативності за рахунок зменшення обчислювальної складності. Серед етапів попереднього оброблення: визначення частини мови слів у тексті, їх нормалізація, видалення “стоп-слів”, виявлення і правильне трактування заперечень.

Окремо звертається увага на необхідність урахування в алгоритмі автоматизації функцій пошуку і виправлення орфографічних помилок.

Отже, зазначені підходи значно збільшують кількість текстів, які підлягають обробленню. Це дозволяє більш об’єктивно формувати узагальнені висновки про інформаційну картину певного періоду часу і, як наслідок, більш адекватно реагувати на ситуацію, прогнозувати розвиток ситуації, працювати на випередження.

Література

1. Sentiment analysis [Електронний ресурс]. – Режим доступу : https://en.wikipedia.org/wiki/Sentiment_analysis. – 25.01.2016.

2. Леонтьева Н. Н. Автоматическое понимание текста: системы, модели, ресурсы / Н. Н. Леонтьева. – М. : Издательский центр «Академия», 2006. – 304 с.

3. Гаспаров Б. М. Язык, память, образ. Лингвистика языкового существования / Б. М. Гаспаров. – М. : Новое литературное обозрение, 1996. – 352 с.

УДК 35-027.21:001.8

Марутян Р.Р.
кандидат історичних наук, доцент,
Національна академія державного управління
при Президентові України

ОРГАНІЗАЦІЙНА ЗБРОЯ У ГІБРИДНІЙ ВІЙНІ

Термін "організаційна зброя" був запропонований в 80-х роках минулого століття в роботах радянських вчених, розробників військових систем організаційного управління С.Никанорова та С.Солнцева. Вони стали

засновниками концепції хибно-цільового програмуванням (ХЦП). Ця назва більш адекватніше відображає глибинну сутність організаційної зброї - сторона-агресор завчасно створює і задає в своїх відносинах із стороною-жертвою помилкові програмні установки, реалізація яких призводить до посилення її позицій і послаблення позицій противника. Противник (майбутня жертва) не сприймає ці програмні установки як небезпечні для нього, тому що вони виглядають нейтральними або такими, що базуються на універсальних цінностях. В сучасних умовах організаційна зброя стала інструментом гібридної війни, в арсеналі якої основними є інформаційні інструменти впливу – від soft power до hard power. Таким чином, сутність організаційної зброї полягає у вживанні «системи організаційних (розвідувальних, пропагандистських, психологічних, інформаційних і ін.) дій на противника, що заставляють його рухатися в необхідному для противника руслі» [2].

Приклади використання організаційної зброї проти України.

Приклад 1. Програмна теза про розвиток економічного співробітництва між Росією і Україною.

М.Азаров: «У економічного співробітництва України з РФ немає альтернативи», «Янукович звернув увагу на важливість подальшого розвитку українo-російського торговельно-економічного співробітництва».

Але, при цьому, російська сторона пропонує відмінний від українського бачення формат співпраці, який передбачає включення України в проекти реінтеграції пострадянського простору - Митний Союз і ЄврАзЕС.

Таким чином, на перший погляд правильна програмна установка на розвиток економічного співробітництва, призводить до стратегічно уразливого положення економіки країни-жертви в разі прийняття противником рішення про агресію: економіка залежна, ослаблена високими цінами на імпорт енергоресурсів і борговими проблемами в відносинах із країною-агресором, не здібна до швидкої переорієнтації на інші ринки тощо.

Приклад 2. Мінські домовленості, дали можливість Росії посилити внутрішню конфліктність в середині суспільства та політичної еліти України. Основний програмний меседж - «Україні і Донбасу потрібний мирний діалог». У реальності призвело фактично до заморожування конфлікту.

Приклад 3. Закон України «Про особливий порядок місцевого самоврядування в окремих районах Донецької та Луганської областей» - вересень 2014 р.

Суспільні ризики, які отримала Україна з прийняттям цього Закону - зміна державного устрою, повна або часткова федералізація України; легалізація квазідержавних утворень в правовому полі України; входження колаборантів та бойовиків у місцеві державні структури (місцева поліція тощо) позачергові парламентські вибори, в результаті яких представники т.зв. «ДНР/ЛНР» можуть отримати мандат депутатів ВР та «блокуючий

пакет» при голосуванні стратегічних законів (наприклад про вступ у НАТО або ЄС), переформатування зовнішньої політики з переорієнтацією на Росію. Кінцевий результат – трансформація України з урізаною територією в нову УРСР.

Використання організаційної зброї у гібридній війні. В сучасній гібридній війні проти України організаційну зброю використовують для впливу на осіб, що приймають рішення (ОПР) з метою ураження системи державного управління. Мета - створення контрольованого управлінського хаосу, руйнування внутрішньополітичної стабільності у державі-мішені, на фоні якого інша держава-сусід виглядатиме осередком прогресу та процвітання, а приєднання до її геополітичних проектів не матиме альтернативи.

Результатом застосування організаційної зброї повинно стати фактично активізація у державі процесів на самоліквідацію. Це деструктивний вплив на державно-управлінські структури держави, знищення системи національної безпеки або її перепрограмування, коли система не ідентифікує загрози та не бореться з ними. Практично з часу отримання Україною Незалежності систему національної безпеки України через кадрові зміни було де-факто переведено в режим зовнішнього управління РФ під контролем російських спецслужб, що створило умови для подальшої збройної агресії. Це також перепрограмування суспільства шляхом смислових та інформаційних впливів на систему національних цінності та заміну її на цінності держави-агресора, у випадку України цінностями "слов'янської єдності" і "російського світу".

Кінцева мета організаційної війни – населення країни-жертви повинно перестати підтримувати владу та представників державних органів влади, звинувачувати у війні та кризі російську владу та керівництво РФ. Виключення раціонального та критичного мислення та гра на емоціях населення.

Одним з інструментів протидії організаційній зброї є формування у населення та державних службовців навиків критичного мислення. Критичність є ознакою зрілого розуму тому за допомогою медіа грамотності треба навчати громадян протистояти ворожої пропаганді. Цій предмет повинен стати обов'язковим у школах та ВНЗ України тому, що саме критичне мислення та об'єктивна картина світу є об'єктом організаційної зброї.

Література

1. Спецслужби РФ дали старт новому антиукраїнському проекту //Дзеркало тижня. 30 травня 2018. – Режим доступу: https://dt.ua/UKRAINE/specsluzhbi-rf-dali-start-novomu-antiukrayinskomu-proektu-is-279164_.html.

2. Султанов Ш. Стратегическое мышление и организационное оружие //Военное обозрение. – 26 августа 2013. – Режим доступу: https://topwar.ru/32397-strategicheskoe-myshlenie-i-organizacionnoe-oruzhie.html.

УДК 342.52
Марущак А.І.
доктор юридичних наук, професор,
Національна академія Служби безпеки України

ДО ПИТАННЯ ПРО ПРЕДМЕТ І МЕТОД ПРАВОВОГО РЕГУЛЮВАННЯ БЕЗПЕКИ ОСОБИ, СУСПІЛЬСТВА, ДЕРЖАВИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Принципом розбудови інформаційного суспільства в Україні є вільний доступ до інформації і знань, крім обмежень, установлених законом. Україна декларує і неухильно дотримується конституційних принципів свободи слова і права на інформацію. Основою методології інформаційного права України у попередніх дослідження автор визначав врегулювання відкритого і обмеженого обігу інформації.

Предметом регулювання інформаційного права є відносини щодо обігу інформації, зокрема її створення, отримання, збирання, зберігання, захисту, використання, поширення тощо. Основними джерелами інформаційного права обґрунтовано визначаємо Закони України «Про інформацію», «Про звернення громадян», «Про доступ до публічної інформації», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про інформаційні агентства», «Про Національний архівний фонд та архівні установи», «Про бібліотеки і бібліотечну справу», «Про державну статистику», «Про державну таємницю», «Про доступ до судових рішень», «Про електронні документи та електронний документообіг», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про кінематографію», «Про науково-технічну інформацію», «Про Національну програму інформатизації», «Про обов'язковий примірник документів», «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про рекламу», «Про систему Суспільного телебачення і радіомовлення України», «Про основні засади забезпечення кібербезпеки України» тощо. Не вирішеною є проблема доцільності правового регулювання суспільних відносин, що виникають з приводу збирання, зберігання, поширення, передачі, знищення інформації за допомогою соціальних мереж.

В умовах зовнішньої агресії проти України виникає наукова і практична проблема визначення меж регулювання відносин щодо безпеки особи, суспільства, держави в інформаційній сфері. Остання конструкція обрана не випадково, а з урахуванням тенденцій розвитку законодавства України (стосовно розмежування інформаційної безпеки і кібербезпеки), а також поглядів науковців на проблему безпеки в інформаційних відносинах (Панченко В.М., Петрова В.В., Лапутіної Ю.А., Ткачука Т.Ю. та інших).

Безпеку особи, суспільства, держави в інформаційній сфері визначаємо одним із видів національної безпеки. Відповідні суспільні відносини як предмет правового регулювання умовно поділяємо на три складові: інформаційна безпека, безпека інформації з обмеженим доступом (далі – ІзОД), кібербезпека.

У більшості правових досліджень йдеться про класичні методи правового регулювання – диспозитивний і імперативний. Л.П.Коваленко у своїх роботах пропонує вважати методом інформаційного права сукупність зафіксованих у нормах цієї галузі прийомів (засобів) впливу на суспільні відносини, що складають її предмет, застосування яких дозволяє створити належні умови для реалізації і захисту прав громадян в інформаційній сфері, нормального функціонування інформаційного суспільства. Однак не зупиняється на особливостях застосування таких методів.

При визначенні методів правового регулювання безпеки особи, суспільства, держави в інформаційній сфері, варто врахувати концептуальну відмінність між регулюванням відносин щодо інформаційної безпеки, де визначальним є протидія негативному інформаційному впливу, щодо обігу ІзОД, за якого визначальною є чітка регламентація процедур створення відповідного організаційно-правового режиму, надання доступу, а також щодо кібербезпеки, пов’язаної із своєчасним виявленням, запобіганням і нейтралізацією реальних і потенційних загроз об’єктам критичної інформаційної інфраструктури.

При забезпеченні інформаційної безпеки переважає диспозитивний метод правового регулювання, оскільки регламентуються процеси обігу переважно відкритої інформації й існує вимога щодо дотримання конституційних принципів свободи слова і права на інформацію, адже учасники таких відносин пов’язані із свободою на вільний вибір форм та способів отримання і поширення інформації. Хоча у цьому напрямку робимо припущення про перспективне посилення юридичної відповідальності за дезінформування як вид інформаційного правопорушення. А відтак і застосування імперативного методу правового регулювання.

При регулюванні безпеки ІзОД метод правового регулювання має бути переважно імперативний, оскільки стосується здебільшого охорони права на таку інформацію.

Відносини з приводу забезпечення кібербезпеки урегульовуються як імперативним (при встановлення технічних вимог щодо захисту державних електронних інформаційних ресурсів), так і диспозитивним, наприклад для унормування питань державно-приватного партнерства.

УДК 347
Мікуліна М.М.
доктор юридичних наук, доцент,
Національна академія Служби безпеки України

ГАРАНТУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ У ГЛОБАЛІЗОВАНОМУ СЬОГОДЕННІ

Стрімке оновлення і трансформація інформаційного простору держави спонукає до усвідомлення, градації кожною особою персональної інформації (даних) щодо себе, її (інформації) співвідношення з правами і свободами людини та меж втручання суб'єктів владних повноважень, фізичних і юридичних осіб в особисту сферу фізичних осіб.

Європейський законодавчий простір констатував, що нормативна база часом вже не відповідає новим викликам, що продемонстрували, зокрема, вихори навколо Cambridge Analytics та Facebook. У Європейському Союзі кілька років поспіль готували новий нормативний акт – Генеральний регламент ЄС про захист персональних даних – GDPR (General Data Protection Regulation), який змінив правила роботи з персональними даними, що є обов'язковими на території ЄС.У ЄС розраховують на те, що зміни забезпечать більший контроль громадянами своїх персональних даних й спростять доступ до них.

Особливістю GDPR є те, що його дія поширюється на всі організації, діяльність яких стосується персональних даних громадян ЄС. Компанії-резиденти ЄС мають партнерів майже в усьому світі, а, отже, новий Регламент застосовуватиметься, зокрема, й в Україні.

Основною особливістю Регламенту є значне розширення прав громадян ЄС щодо контролю своїх персональних даних. Зокрема, згідно з новим Регламентом громадяни країн-членів ЄС можуть робити запити щодо: підтвердження факту обробки їх даних; місце і мету обробки; категорії оброблюваних персональних даних; третіх осіб, яким персональні дані надаються; період, протягом якого дані обробляються; уточнення джерела отримання даних; вимоги виправлення даних; вимоги припинення обробки даних; видалення даних (право бути забутим або видаленим).

Основними принципами обробки персональних даних згідно з GDPR є: 1) законність, справедливість і прозорість (інформація про мету, методи та обсяги обробки є максимально доступною і простою); 2) обмеження застосування (персональні дані збираються і використовуються винятково відповідно до мети); 3) мінімізація даних (заборона на збирання даних в більшому обсязі, ніж зазначено у меті); 4) точність (неточні дані підлягають виправленню або видаленню – на вимогу користувача); 5) обмеження зберігання (дані зберігаються у формі, що дозволяє ідентифікувати суб'єкта даних на строк, що не перевищує мету обробки); 6) цінність і конфіденційність (обов'язок володільця даних забезпечити захист персо-

нальних даних від їх несанкціонованої чи незаконної обробки, пошкодження та знищення).

Новий Регламент містить певні вимоги до накопичення, збереження, обігу, безпеки персональних даних [1]. Зокрема, статті 5, 25, 32 GDPR містять вимоги до організацій;конфіденційність гарантується статтями 6, 25, 28, 32; право на видалення – статтями 17 і 28; профілактика ризиків та комплексної перевірки - статтями 2, 24, 28; також передбачено також право фізичної особи на доступ до її персональних даних протягом одного місяці з дня надіслання відповідного запиту, за певних умов цей строк може бути збільшений на два місяці; обов'язок організацій щодо повідомлення про порушення, викладені у статтях 33 і 34. Усі ці вимоги до безпеки персональних даних стосуються даних, що зберігаються, обробляються у фізичному та віртуальному дата-центрі, так і тих, що перебувають у «хмарних сховищах».

Передбачаються також санкції за порушення GDPR, що полягають у: попередженні у письмовій формі у випадках першого і ненавмисного недотримання; регулярних періодичних перевірках захисту даних; штрафах до 10 млн. євро або 2% щорічного світового обігу, а також до 20 млн євро або 4% щорічного світового обігу [2].

Державні органи, а також підприємства, основна діяльність яких стосується регулярного чи систематичного опрацювання персональних даних, зобов'язані упровадити посаду співробітника з питань захисту даних, який відповідатиме за дотримання GDPR.

Безперечно, що такі єдині наддержавні стандарти захисту персональних даних забезпечать високий рівень охорони персональних даних у всіх сферах життєдіяльності, убезпечать процес міжнародного переміщення персональних даних, а також функціонування цього інституту у кожній державі.

Узагальнивши існуючий позитивний міжнародний досвід щодо правових стандартів функціонування інституту персональних даних та персональної інформації, можливе й доцільне внесення змін, доповнень до законодавчих актів України у цій сфері. «Включення питання щодо приведення українського законодавства у відповідність до Регламенту до проекту змін до Плану дій з реалізації Національної стратегії у сфері прав людини на період до 2020 року свідчить про важливість європейського документу для забезпечення захисту прав людини в Україні» [3].

Література

1. Нужний В. Нові вимоги ЄС до захисту персональних даних з травня 2018 року. – Режим доступу: Channel4it/com.

2. Kadrovik/ua.

3. Ukrainepravo/com.

УДК 355.01:341.322
Морозов О.М.
доктор медичних наук, професор,
Національна академія Служби безпеки України
Морозова Т.Р.
доктор психологічних наук,
старший науковий співробітник,
Національна академія Служби безпеки України

ОСНОВИ СТРАТЕГІЇ НАСТУПУ ТА ЗАХИСТУ В ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІЙ БОРОТЬБІ

Розглянемо основні елементи передумов, організації та методів боротьби в інформаційно-психологічному просторі. Особливості менталітету окремої людини або населення, котре буде піддаватися маніпулюванню, відіграють значну роль у розробці програми психологічного впливу.

Для досягнення ефективного, часто руйнівного, психологічного впливу на масу необхідне послідовне вирішення низки основних завдань:

- створення власного інформаційного простору на території, яка підлягає психологічному впливу;
- максимального обмеження доступу будь-якої несанкціонованої інформації на таку територію шляхом пригнічення, а при можливості і повного знищення її джерел (технічних, людських), занурення населення у інформаційний простір визначеного змісту;
- максимальне обмеження вільного пересування людей за межі зони, що піддається інформаційній обробці, а за неможливості повного обмеження пересування людей, організація джерел психологічного впливу у місцях найбільшого скупчення осіб, котрі тимчасово виїхали за межи зони психологічної обробки;
- інформаційна, а за можливості і фізична ізоляція, дискредитація і «демонізація» (формування негативного образу), а за неможливості контролю й нейтралізація небажаних лідерів противника, що мають вплив на маси;
- організація безперервного радіо- і телемовлення, випуску друкарської продукції, насичення Інтернету необхідною інформацією, брутальною брехнею, витонченими фейками, розповсюдження чуток необхідного змісту;
- пошук серед населення що обробляється осіб, схильних до різних форм співробітництва із противником («корисні ідіоти», зрадники, агенти впливу) та інтенсивне створення їм образу борців за щастя народу і поширення через них необхідної інформації;
- створення винятково позитивного, героїчного, фантастичного, недосяжного образу агресора, особливо його провідників і у першу чергу харизматичного, непереможного, могутнього вождя, генія і полководця;

- створення у населення, котре піддається обробці, комплексу нікчемності, неповноцінності, ізоляції, ідей самознищення, почуття провини, формування тривожно-депресивного стану, неминучої необхідності і доцільності скоритися агресору – «визволителю».

Серед етапів і прийомів навіювання необхідної інформації через ЗМІ можна навести такі:

- етап занурення. Використовуючи спеціально розроблені аудіо, візуальні, аудіовізуальні інформаційні ряди, привчити населення до засобів масової інформації як до чогось звичного, повсякденного, без чого неможливо обійтися. Відмінною рисою цих інформаційних програм є їхня легкість для сприйняття, поверхневість, банальність. Вони привчають людей бездумно сприймати практично будь-яку інформацію. Прикладами таких програм, які сплощують людську психіку і усувають критику, є численні безкінечні телесеріали, просякнуті прихованою пропагандою, цілодобові радіопрограми, на яких пропонують примітивну і цілком одноманітну музику, серії цілеспрямованих газетних статей;

- етап маніпулювання. Після підготовки, що нівелює психіку населення, знижує критику і відкриває «ворота навіюваності», повинні з'являтися програми, розраховані на маніпулювання суспільною свідомістю. Головним дієвим чинником таких програм є неправда, яка подається брутально або різноманітними витонченими способами. Брехливу інформацію необхідно не тільки виготовити відповідним чином, але і подати у формі, зручній для сприйняття. Крім того, людина, котра подає цю інформацію, також повинна мати благовидний вигляд і викликати довіру. В цілому найбільш ефективною є пряма брутальна брехня, яка повторюється тривалий час та з різних джерел;

- етап управління. Занурення в інформаційне поле, що складається із суцільно регульованих потоків неправди, здійснюється за рахунок прямої брутальної брехні – для швидкого вирішення короткострокових завдань; брехні, яка подається за допомогою спеціальних лінгвістичних прийомів – для вирішення середньострокових завдань; і брехні, що супроводжується «науковим обґрунтуванням», історичними екскурсами, яскравими, такими, що подаються у перекрученому вигляді, прикладами, думкою фальшивих авторитетів, які є, як правило, спеціально підготовленими людьми, психічно неврівноваженими або схильними до співробітництва із противником особами – для досягнення довгострокової мети;

- етап пригнічення. Потужним важелем психологічного впливу на масу є релігійна пропаганда. Впровадження у свідомість маси ідеї смиренності, самообмеження, пошуку щастя в загробному світі, перекручене тлумачення релігійних догматів і формування образу ворога, нав'язування ідей і дій в інтересах агресора, перетворює людей у легко керовану агресивну масу;

- технічне забезпечення. Весь комплекс інформації, розрахований на маніпулювання суспільною свідомістю, подається з використанням фізіологічних і психологічних законів її сприйняття. Використовуються спеціально змонтовані відеоряди, особлива побудова текстів, особливий темп і модуляції мовлення. Маніпулювання через використання субсенсорних механізмів сприйняття аудіовізуальної інформації представляє з себе суто технічний вплив на підсвідомість людини з метою спрямування думок і діяльності в потрібному напрямку. Серед значної кількості субсенсорних прийомів найбільш старим і відомим широкому загалу є так званий 25 кадр.

Що стосується протидії масовому психологічному впливу через ЗМІ, то важливим фактором зміцнення національної безпеки держави та позитивного розвитку громадянського суспільства є розробка чіткої та послідовної програми побудови та розвитку засобів масової інформації, створення відповідного інформаційного простору на теренах держави та за її межами. Серед основних завдань можна виокремити наступні:

1. Розробка і впровадження заходів щодо захисту від негативного психологічного впливу населення і провідників держави.

2. Формування і впровадження на теренах держави єдиної державницької національної ідеї.

3. Формування загальнодержавних проектів політичного, економічного та соціального спрямування.

4. Налагодження регулярного інформаційно-психологічного супроводження стратегічних політичних, економічних та соціальних проектів в середині держави та на міжнародній арені.

5. Проведення моніторингу соціально-психологічного стану у державі.

6. Визначення найбільш актуальних соціально-психологічних проблем.

7. Розробка рекомендацій з подолання соціально-психологічних ускладнень.

8. Розробка рекомендації з попередження соціально-психологічних ускладнень.

9. Розробка рекомендації з впровадження в суспільство розроблених рекомендацій.

10. Проведення моніторингу ефективності впровадження розроблених рекомендацій з оптимізації соціально-психологічного стану в державі.

11. Створення в світовій спільноті позитивного іміджу держави.

УДК 351.861
Пилипчук В.Г.
доктор юридичних наук, професор,
член-кореспондент Національної академії
правових наук України,
Науково-дослідний інститут
інформатики і права НАПрН України

РОЗВИТОК СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ, СУСПІЛЬСТВА І ДЕРЖАВИ

В умовах поширення новітніх інформаційних технологій, створення державних і недержавних реєстрів, інформаційних систем і баз даних, формування національного і глобального інформаційного простору та розвитку інформаційного суспільства проблема захисту персональних даних стає однією із ключових в системі захисту прав і безпеки людини.

Правозастосовна практика у цій сфері в Україні залишається досить неоднозначною. Нині питання захисту персональних даних викликає занепокоєння у значної кількості громадян України у зв'язку з можливістю незаконного поширення і несанкціонованого використання цих даних. Незважаючи на наявність правового механізму захисту персональних даних *(Конституція України, міжнародні стандарти, «Пакет захисту даних ЄС», Закон України «Про захист персональних даних»)*, у реальному житті його ефективність є досить сумнівною. Об'єктивно, це може визначатися труднощами політико-правових та соціально-економічних трансформацій, що відбуваються в Україні. З іншого боку, поширеною є думка, що проблеми захисту персональних даних не відносяться до найбільш актуальних в сучасних умовах. При цьому не береться до уваги той факт, що нині немає жодної сфери життєдіяльності людини, суспільства і держави, де не оброблялися б персональні дані.

Крім цього, положення Закону України «Про захист персональних даних» є далекими від досконалості. Зокрема, необхідним є створення дієвого механізму захисту права людини на власні персональні дані, удосконалення понятійно-категоріального апарату, запровадження механізму встановлення суб'єктом персональних даних режиму конфіденційності своїх даних, удосконалення галузевого законодавства (охорона здоров'я, освіта тощо), яке в тій чи іншій мірі регулює питання захисту персональних даних у конкретній сфері життєдіяльності людини тощо.

Як свідчать результати дослідження [1], базові закони про захист персональних даних у більшості європейських країн були прийняті наприкін-

ці XX – на початку XXI століття. Незважаючи на розходження правових систем, в основу законодавства про захист персональних даних покладено однакові принципи, викладені в міжнародних стандартах. Захист персональних даних розглядається у політичних системах різних країн європейського континенту як невід'ємний елемент демократії та правової держави. Більшість законів європейських країн у сфері захисту персональних даних мають типову назву – закон про захист даних. Під ***«захистом даних»*** (data protection) розуміють будь-які правові, організаційні, технічні (технологічні, криптографічні, програмні) засоби щодо захисту інформації персонального змісту. Для комплексного захисту даних на міжнародному рівні використовується термін ***«безпека даних»*** (data security).

Розробку ідеї про необхідність розгляду сукупності інформації про фізичну особу як об'єкта правової охорони одними з перших розпочали американські правознавці. Розвиток цієї ідеї знайшов відображення у так званій концепції ***«права на приватність»*** (right to privacy) – ***права особи «на саму себе», права «бути залишеною на самоті»*** (privacy) [2-3]. За матеріалами узагальнення прецедентної практики в США [4] *«делікти проти приватності»* (privacy torts) було розділено на такі групи:

– втручання в усамітненість (intrusion upon seclusion) – вторгнення в «особистий простір» індивіда;

– публічне розголошення інтимних фактів (publication of private facts);

– спотворене представлення особи перед громадськістю (false light);

– використання чужого імені або образу в корисливих цілях (appropriation).

Головним правовим стандартом, що встановив принципи гармонізації національних законодавств у сфері захисту персональних даних є Конвенція Ради Європи від 28.01.1981 р. № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [5], до якої приєднались усі держави-члени ЄС. Зазначений міжнародно-правовий договір прийнято з урахуванням стрімкого зростання в ЄС транскордонного потоку персональних даних. Згідно з Конвенцією № 108 *збирання, накопичення, зберігання і поширення персональних даних може здійснюватися* ***лише з дозволу особи, дані про яку обробляються***. *Цій* ***особі*** *надано право* ***знати місце роботи та проживання володільця персональних даних (відповідального за обробку даних)****, а також право отримувати відповідні дані без затримки та у зрозумілій формі.* Вказаний акт також заклав підґрунтя до формування національних систем захисту персональних даних, у т.ч. в Україні.

У травні 2016 року Європейський Парламент і Рада затвердили постанову про нові правила і порядок захисту персональних даних ***(«Пакет захисту даних»***) [6], який набув чинності у травні 2018 р., передбачає створення узгодженої нормативно-правової бази у державах-членах ЄС та

рекомендований до впровадження іншими країнами, що співпрацюють з ЄС. Він включає наступні документи:

– Регламент (ЄС) 2016/679 від 27.04.2016 р. «Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальні Положення про захист даних)»;

– Директиву (ЄС) 2016/680 Європейського Парламенту і Ради від 27.04.2016 р. «Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами в цілях запобігання, розслідування, виявлення або переслідування злочинця злочину або виконання кримінальних покарань, а також про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/ПВД»;

– Директиву (ЄС) 2016/681 Європейського Парламенту і Ради від 27.04.2016 р. «Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину».

Слід зауважити, що стаття 17 вказаного Регламенту закріплює за суб'єктом персональних даних «***право бути забутим***» («right to be forgotten»). Крім того, ця стаття додатково уточнює право на видалення даних і визначає умови використання «права бути забутим», включаючи *обов'язок володільця, який оприлюднив персональні дані, повідомляти треті сторони про вимогу суб'єкта даних щодо усунення будь-яких посилань на відповідні персональні дані, а також видалення будь-яких копій чи примірників таких персональних даних.* Вона також передбачає право на обмеження обсягів обробки в певних випадках, уникаючи при цьому використання двозначного терміну «блокування даних». Значна увага у тексті Регламенту приділяється питанню ***захисту безпеки персональних даних*** і так званій «*оцінці впливу захисту даних»*, що полягає в *обов'язку для володільців та розпорядників персональних даних проводити попередню оцінку захисту даних до проведення ризикованих операцій з їх обробки*.

Основні принципи обробки персональних даних, наведені у документах «Пакета захисту даних», визначають додержання таких вимог:

– персональні дані повинні оброблятися законно, справедливо і в доступній формі по відношенню до суб'єкта даних («законність, справедливість і прозорість»);

– збиратися для певної, конкретної і законної мети і не піддаватися додатковій обробці, яка несумісна з цією метою; подальша обробка для цілей архівації, з метою наукових, дослідницьких, історичних і статистичних цілей не може бути несумісною з початковою метою («цільове обмеження»);

– бути адекватними і обмежуватися тими даними, які відповідають і необхідні для досягнення цілі, для яких вони обробляються («зведення до мінімуму даних»);

– бути точними і, при необхідності, постійно підтримуватися в актуальному стані; неточні персональні дані, з урахуванням цілі, для якої вони обробляються, слід видаляти або виправляти без затримки («точність»);

– зберігається у формі, що дозволяє ідентифікувати суб'єкта даних не довше, ніж це необхідно для цілі, для якої вони обробляються; персональні дані можуть зберігатися протягом тривалішого періоду виключно для цілей архівації, інтересів наукових, дослідницьких, історичних і статистичних цілей («обмеження зберігання»);

– обробляються так, щоб забезпечити належний захист персональних даних, включаючи захист від несанкціонованої або незаконної обробки, випадкової втрати, знищення або пошкодження, з використанням відповідних технічних або організаційних заходів («цілісність і конфіденційність»).

Широке використання технологій ***Інтернету речей, «хмарних технологій», «Великих Даних»*** призводить до необхідності забезпечення інформаційної безпеки та вирішення таких основних правових проблем:

– визначення механізмів реалізації принципу попередньої згоди на використання та вилучення персональних даних;

– правового впливу на регулювання транскордонних потоків персональних даних, що передбачає не тільки цілеспрямовану діяльність щодо впорядковування інформаційних відносин, але і непряму дію правових засобів і методів на різних суб'єктів, які безпосередньо не підпадають під правове регулювання;

– врегулювання порядку використання персональних даних інтелектуальними комплексами, що функціонують без участі суб'єктів (юридичних або фізичних осіб);

– необхідності створення багаторівневої і багато об'єктної системи захисту персональних даних, що потребує формування нової системи правового регулювання.

В цілому, результати дослідження правових стандартів захисту персональних даних у законодавстві Європейського Союзу та реального стану захисту персональних даних в Україні дають змогу дійти низки ***загальних висновків***:

– персональні дані, як найбільш чутлива і важлива для людини інформація, посідають особливе місце в інформаційних відносинах та системі інформаційної безпеки людини, суспільства і держави;

– наявна система захисту персональних даних в Україні не гарантує захисту приватності та персональних даних людини і громадянина, не від-

повідає низці положень Конституції України та потребує приведення у відповідність до правових стандартів ЄС;

– ***основні принципи захисту персональних даних***, наведені у «Пакеті захисту даних ЄС», передбачають обов'язкове дотримання конкретних умов їх застосування, зокрема, будь-яка обробка персональних даних повинна здійснюватися законно, бути справедливою і прозорою для суб'єкта даних, та виконуватися лише згідно з конкретно визначеною метою;

– впровадження інституту ***права приватної власності людини на свої персональні дані*** в умовах стрімкого розвитку інформаційних технологій та їх нових можливостей для тотального контролю за приватним життям людини може надати найбільш реальні правові гарантії захисту персональних даних, що потребує додаткового теоретичного і правового опрацювання;

– проблема неправомірних і несанкціонованих дій у сфері захисту персональних даних фізичних осіб в Україні залишається вкрай актуальною в юридичному і практичному відношенні, а чинне законодавство у цій сфері потребує кардинального перегляду в контексті євроінтеграції України.

Загалом, актуальною постає ***проблема розробки і впровадження нової системи захисту персональних даних***, основними складовими якої можуть бути:

1) затвердження *Верховною Радою України* ефективної державної політики з питань захисту персональних даних та розвиток парламентського контролю у цій сфері відповідно до стандартів ЄС;

2) системне задіяння для захисту персональних даних комплексу правових, організаційних і технічних заходів, перегляд завдань, функцій та повноважень відповідних державних органів та органів місцевого самоврядування;

3) створення інституту *Уповноваженого з питань захисту персональних даних*, підзвітного Верховній Раді України, основними функціями якого можуть бути забезпечення нагляду і контролю та удосконалення нормативно-правової бази з питань захисту персональних даних, а також взаємодія з уповноваженими органами ЄС та країн-членів ЄС з питань захисту даних;

4) покладання на центральні органи виконавчої влади згідно з їх компетенцією виконавських функції з питань захисту персональних даних. Зокрема, вивчення питання щодо створення окремого функціонального підрозділу у складі апарату *Міністерства юстиції України* і його територіальних органів або відновлення *Державної служби з питань захисту персональних даних*, діяльність якої скеровуватиметься через Мін'юст України;

5) покладання на *Державну службу спеціального зв'язку і технічного захисту інформації України* функцій організації забезпечення технічного захисту персональних даних в Україні;

6) віднесення до компетенції *Державного бюро розслідувань України* проведення досудового слідства щодо правопорушень, які стосуються захисту персональних даних, а також покладання на *Національну поліцію України* функції сприяння у проведенні перевірок та розслідування правопорушень у цій сфері;

7) опрацювання питання *(з урахуванням п. 20 Преамбули Регламенту (ЄС) 2016/679, що його правила застосовуються у діяльності судів та інших судових органів, а також досвіду Суду із захисту даних Великої Британії)* про створення окремих судових палат у складі апеляційних судів і Верховного Суду України або створення спеціалізованого суду з питань захисту інформації (даних) з можливим покладанням на вказані органи розгляду справ щодо *порушення права приватності життя людини і захисту персональних даних, правопорушень у сфері обігу інформації, надання доступу до публічної інформації, діяльності засобів масової інформації та використання інформаційно-комунікаційних систем і мереж, єдиних державних реєстрів та інформаційних ресурсів, роботи з інформацією, що становить державну таємницю або містить відомості з обмеженим доступом*;

8) запровадження в органах, установах, закладах, підприємствах та організаціях *(згідно з нормами ЄС)* посад фахівців з питань захисту персональних даних або покладання цих функцій на окремих працівників цих організацій.

Загалом, реалізація зазначеного сприятиме усуненню системних проблем щодо захисту персональних даних, впровадженню у національне законодавство визначених законодавством Європейського Союзу стандартів і механізмів у цій сфері, а також підвищенню інформаційної безпеки людини, суспільства і держави.

Література

1. *Пилипчук В.Г., Брижко В.М., Баранов О.А.* та ін. Становлення і розвиток правових основ та системи захисту персональних даних в Україні : монографія / В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник; за заг. ред. Брижка В.М., Пилипчука В.Г. – К. : ТОВ «Видавничий дім «АртЕк», 2017. – 226 с.

2. *Уоррен С., Брандейс Л.* Право на приватность // Право США. – № 1-2/2013. – С. 151-152.

3. Рішення Верховного Суду штату Джорджія у справі «Павєсіч vs. Нью Ігленд Лайф Іншуранс Ко.» від 1905 р. (Pavesich vs. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905)) // Information privacy law: Textbook / D.J. Solove, M. Rotenberg. – New York: Aspen Publishers, 2003. – 795 p.

4. *Bennett C.J., Raab C.D.* Taking the Measure of Privacy: Can Data Protection be Evaluated? // International Review of Administrative Sciences. – 1996. – № 4 (62). – P. 31-32.

5. Конвенція Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 1981 р. № 108 // Офіційний вісник України. – 2011. – № 1. – С. 701; Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних // Офіційний вісник України. – 2011. – № 1. – С. 708.

6. *Брижко В.М.* Сучасні основи захисту персональних даних в європейських правових актах // Інформація і право. – № 3(18)/2016. – С. 45-57.

УДК 343.123

Пічкуренко С. І.
кандидат юридичних наук, доцент,
Національна академії внутрішніх справ
Кацан Л.О.
Національна академії внутрішніх справ

МІСЦЕ І РОЛЬ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

У комплексі заходів, які проводяться органами державного управління у сфері національної безпеки України, на нашу думку, важливу роль належить підрозділам Національної поліції України, які є найчисленніші серед правоохоронних органів України.

Сьогодні діяльність Національної поліції у сфері забезпечення національної безпеки носить досить складний характер. У механізмі держави вони не є спеціальними органами, покликаними безпосередньо гарантувати належний рівень національної безпеки. Але під час виконання підрозділами Національної поліції завдань передбачених законом України «Про Національну поліцію України», щодо забезпечення публічної безпеки і порядку, охорони прав і свобод людини, а також інтересів суспільства і держави, боротьбі зі злочинністю, останні протидіють широкому колу загроз національної безпеки, зокрема, організованій та кіберзлочинності, які несуть реальну загрозу у сфері інформаційної безпеки України. Члени організованих груп та злочинних організацій нерідко залучають до своєї діяльності представників правоохоронних органів, які порушують вимоги закону «Про державну таємницю».

Слід зазначити, що певна увага окремим аспектам досліджуваної теми приділена у працях В. Абрамова, В. Білоуса, В. Богдановича, В. Горбуліна, А. Дацюка, О. Дзьобана, І. Завидняка, А. Качинського, О. Ліпкана, Р. Марутяна, О. Масензова, Р. Мошинського, Н. Нижник та інших дослідників [1], які висвітлюють загальні питання забезпечення національної безпеки України.

Серед органів і підрозділів Національної поліції України суб'єктами протидії організованій та кіберзлочинності є оперативні підрозділи кримінальної поліції.

До блоку кримінальної поліції входять підрозділи карного розшуку, стратегічних розслідувань, боротьби зі злочинами, пов'язаними з торгівлею людьми, оперативної служби, оперативно-технічних заходів, виявлення небезпечних матеріалів та екологічних злочинів, протидії наркозлочинності (межрегіональний підрозділ). внутрішньої безпеки (міжрегіональний підрозділ), кіберполіції (межрегіональний підрозділ), захисту економіки [2].

Аналіз відомчих нормативно-правових актів, щодо оперативно-розшукової та оперативно-службової діяльності вказаних підрозділів свідчить, що кожен з них здійснює комплекс оперативно-розшукових заходів у різних сферах життєдіяльності нашої держави, серед яких головними є: охорона прав і свобод людини, інтересів суспільства і держави, протидії злочинності, виявлення і розкриття злочинів загально-кримінальної спрямованості, розшук осіб, які їх учинили, документування протиправної діяльності учасників та членів організованих груп і злочинних організацій; забезпечення реалізації державної політики щодо захисту економіки та об'єктів права власності, виявлення, запобігання та припинення злочинів у сфері економіки, у тому числі вчинених суспільно-небезпечними організованими групами та злочинними організаціями, які впливають на соціально-економічну і криміногенну ситуацію в державі та в окремих її регіонах, боротьба з корупцією й хабарництвом у сферах, які мають стратегічне значення для економіки держави та серед посадових осіб органів державної влади і самоврядування; протидія корупційним правопорушенням і правопорушенням, пов'язаним з корупцією; забезпечення реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; попередження та виявлення небезпечних (радіаційних, хімічних, біологічних, ядерних) матеріалів та пов'язаних з ними екологічних злочинів; забезпечення реалізації державної політики у сфері протидії кримінальним правопорушенням, пов'язаним з торгівлею людьми, нелегальною міграцією, правопорушеннями у сфері суспільної моралі; розробка та реалізація програм протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та запобігання поширенню наркоманії, організація та проведення оперативно-розшукових заходів із виявлення і документування тяжких та особливо тяжких кримінальних правопорушень, пов'язаних з незаконним обігом наркотичних засобів, психотропних речовин і прекурсорів, насамперед учинених злочинними групами осіб, які мають міжрегіональні та міждержавні зв'язки, особливо в їх організованих формах [3].

Саме діяльність цих підрозділів є надійною гарантією протидії злочинності, створення реальних умов для нормального функціонування

держави, захисту її національних інтересів, в тому числі у сфері інформаційної безпеки України.

Одним із засобів у протидії реальним загрозам інформаційній безпеки Україні, на нашу думку є використання оперативними підрозділами оперативно-розшукових форм, методів, засобів та оперативно-розшукових заходів, передбачених чинним законодавством України [4].

Література

1. Проблеми забезпечення національної безпеки України на сучасному етапі державотворення : матеріали круглого столу (Київ, 21 жовт. 2010 р.) ; НАДУ при Президентові України ; за заг. ред. Г. П. Ситника. – К. : НАДУ, 2011. – 72 с

2. Структура апарату Національної поліції [Електронний ресурс]. – Режим доступу: https://www.npu.gov.ua/.

3. Закон України «Про Національну поліцію» // Документи Верховної Ради України : [сайт] – Режим доступу: http://zakon.rada.gov.ua.

4. Закон України «Про оперативно-розшукову діяльність» // Документи Верховної Ради України : [сайт]. – Режим доступу: http://zakon.rada.gov.ua.

5. Закон України «Про організаційно-правові основи боротьби з організованою злочинністю» // Документи Верховної Ради України : [сайт] — Режим доступу: http://zakon.rada.gov.ua.

УДК 004.056

Полотай О.І.
кандидат технічних наук, доцент,
Львівський державний університет безпеки життєдіяльності
Рожко Д.К.
Львівський державний університет безпеки життєдіяльності

ПРИНЦИПИ ТА ПОРЯДОК РОЗРОБЛЕННЯ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Те, що інформація має цінність, люди усвідомили дуже давно. Її створюють, зберігають, транспортують, продають і купують, а значить - крадуть і підробляють - і, отже, її необхідно захищати. Одним словом, виникнення індустрії обробки інформації призвело до виникнення розробки засобів захисту інформації. Забезпечення безпеки інформації у інформаційно-телекомунікаційних системах здійснюється шляхом створення та впровадження комплексних систем захисту інформації.

Комплексна система захисту інформації – це сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації від несанкціонованого доступу.

В Законі України «Про захист інформації в інформаційно-телекомунікаційних системах визначено: «Інформація, яка є власністю держави або інформація з обмеженим доступом, вимога щодо якості якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації (далі – КСЗІ) з підтвердженою відповідністю».

Роботи зі створення КСЗІ виконуються організацією-власником ІТС. За умови відсутності у неї відповідних ліцензій або дозволу на здійснення окремих видів робіт із захисту інформації до виконання цих робіт залучаються суб'єкти господарювання, які мають такі ліцензії. Дозвіл на проведення робіт з технічного захисту інформації для власних потреб дається Державною службою спеціального зв'язку та захисту інформації.

Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розробку і впровадження інформаційної технології, що забезпечує обробку інформації в ІТС згідно з вимогами, встановленими державними стандартами, нормативно-правовими актами та нормативними документами у сфері захисту інформації. Для створення КСЗІ використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та криптографічного захисту інформації.

До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

1. Витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;

2. Несанкціонованих дій та несанкціонованого доступу до інформації

3. Спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Створення комплексів технічного захисту інформації від витоку технічними каналами здійснюється, якщо в ІТС обробляється інформація, яка становить державну таємницю або коли необхідність цього визначена власником інформації.

Етапи створення КСЗІ:

1 етап. Обстеження ІТС та підготовка вихідних даних для формування вимог до КСЗІ;

2 етап. Формування політики безпеки;

3 етап. Розробка технічного завдання на створення КСЗІ;

4 етап. Розробка і реалізація проекту КСЗІ в ІТС;

5 етап. Введення КСЗІ в дію;

6 етап. Попередні випробування;

7 етап. Дослідна експлуатація;

8 етап. Державна експертиза КСЗІ;

9 етап. Супровід КСЗІ.

Під політикою безпеки інформації в Системі розуміється набір законів, нормативних документів, вимог, правил, обмежень, інструкцій, рекомендацій, що регламентують порядок обробки інформації і спрямовані на захист інформації від визначених погроз. Програмна політика безпеки – є політикою вищої ланки управління в організації. Об'єктом є організація в цілому, за розробку і здійснення програмної політики несе відповідальність керівництво організації. Програмна політика визначає стратегічні напрямки забезпечення інформаційної безпеки.

Політика безпеки повинна передбачати комплексне використання правових і морально-етичних норм, організаційних (адміністративних) мір, фізичних, технічних (апаратних і програмних) способів і засобів захисту інформації, а також визначати правила і порядок їхнього застосування в Системі

Методологія розробки політики безпеки містить у собі наступні роботи: розробка концепції безпеки інформації в Системі; аналіз ризиків; визначення вимог до методів і засобів захисту; вибір основних рішень по забезпеченню безпеки інформації; організація виконаних робіт і забезпечення безупинного функціонування Системи; документальне оформлення політики безпеки.

Отже, потрібно чітко розуміти, що будь-які засоби захисту інформації не гарантують абсолютну безпеку і надійність даних, проте вони суттєво мінімізують ризик втрат. При проведенні аналізу та об'єктивної оцінки фахівець з інформаційної безпеки повинен забезпечити найефективніші методи та засоби створення комплексної системи захисту інформації.

Література

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 року;

2. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-2005.

УДК 340.5; 351
Прощаєв В.В.
кандидат юридичних наук, доцент,
Інститут Служби зовнішньої розвідки України

ЗАКОНОДАВЧІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СФЕРІ ДІЯЛЬНОСТІ РОЗВІДУВАЛЬНИХ ОРГАНІВ РЕСПУБЛІКИ БІЛОРУСЬ

Інформаційна безпека у сфері функціонування зовнішньої розвідки Республіки Білорусь (РБ) визначена правовими приписами у низці законодавчих актів. Це цілком зрозуміло, бо керівництво РБ, як й інших держав – учасників СНД, ставить перед зовнішньою розвідкою завдання щодо добування розвідувальної інформації негласними силами і засобами та виключно притаманними розвідці таємними методами, натомість в інформаційних базах, створюваних органами розвідки, концентруються дуже важливі відомості та інформація, що становлять державну таємницю вищого ступеня секретності.

На законодавчому рівні у Законі РБ «Про державні секрети» визначено перелік відомостей у сфері розвідувальної діяльності, які обов'язково мають бути віднесені до державної таємниці, а саме:

відомості про організацію, тактику, сили, засоби, об'єкти, методи, плани розвідувальної діяльності, в тому числі щодо забезпечення власної безпеки у розвідувальних органах, що здійснюють таку діяльність;

про фінансування заходів, що проводяться розвідувальними органами;

про громадян, що надають (надавали) на конфіденційній основі сприяння органам, що здійснюють розвідувальну діяльність, а також про штатних негласних співробітників і співробітників цих органів, в тому числі впроваджених в організовані групи, які виконують (виконували) спеціальні завдання.

Крім загальних Законів РБ «Про державні секрети» та «Про інформацію, інформатизацію та захист інформації», Указу Президента РБ про затвердження «Переліку відомостей, що становлять державну таємницю Республіки Білорусь», в яких правовими нормами визначено загальні питання збереження та поводження з таємною інформацією у державних органах, у тому числі й розвідувальних, саме Президент РБ вважав за необхідне у своєму Указі «Про питання зовнішньої розвідки» від 25 березня 2003 р., № 116 визначити деякі правові засади управління інформаційною безпекою у діяльності зовнішньої розвідки, а саме:

споживачі розвідувальної інформації для прийняття на її підставі виважених політичних або державних рішень (керівники уряду, інших державних органів, члени Ради безпеки РБ) підлягають відповідальності відповідно до чинного законодавства за розголошення відомостей, що стано-

влять державну таємницю та знаходяться у наданій їм розвідкою інформації;

розвідувальні органи мають право вжиття заходів щодо легендування співробітників розвідувальних служб та організації їх діяльності з використанням у цих цілях іншої відомчої належності;

керівники розвідувальних органів мають право вносити в установленому порядку пропозиції про створення організацій прикриття або їх підрозділів, необхідних для виконання завдань зовнішньої розвідки;

співробітники розвідувальних служб для виконання своїх обов'язків можуть займати посади в інших державних органах або організаціях.

Необхідно зазначити, що білоруський законодавець на відміну від російського дуже поверхово визначив в основному нормативно-правовому акті про діяльність зовнішньої розвідки питання забезпечення її інформаційної безпеки. Не знайшли свого відображення правові приписи про такі важливі моменти:

виготовлення та використання документів прикриття, що зашифровують особистість співробітників кадрового складу, відомчу належність підрозділів, організацій, приміщень та транспортних засобів до органів зовнішньої розвідки;

розроблення, створення та експлуатацію власних інформаційних систем, систем зв'язку і передачі даних, а також засобів захисту інформації від її витоку по технічним каналам;

проходження особою, що допускається до відомостей про органи зовнішньої розвідки, обов'язкової процедури оформлення допуску до державної таємниці;

створення органами зовнішньої розвідки власних архівів та можливість передачі документі на постійне збереження до державної архівної служби після їх розсекречування відповідно до чинного законодавства;

зберігання документів, що містять відомості про кадровий склад, про осіб, які сприяють (сприяли) на конфіденційній основі органам розвідки, а також про методи і засоби розвідувальної діяльності виключно в архівах органів зовнішньої розвідки.

Також, на відміну від законодавства Російської Федерації в Указі Президента РБ жодного слова немає про можливість та порядок опублікування матеріалів про зовнішню розвідку у засобах масової інформації. Немає правових приписів щодо надання органам розвідки права на розробку та видання спеціальних закритих відомчих нормативно-правових актів, у яких визначався б порядок використання негласних методів та засобів розвідувальної діяльності, можливість ведення справ тощо. Для забезпечення інформаційної безпеки суттєве значення мав би правовий припис про фінансування та матеріально-технічне забезпечення органів зовніш-

ньої розвідки, про державний орган, в якому розглядалися б та затверджувалися б проекти кошторисів витрат на утримання органів розвідки.

В Указі Президента РБ визначено деякі соціальні гарантії особам, які сприяють (сприяли) на конфіденційній основі органам розвідки, але не зазначено, що відомості про цих осіб становлять державну таємницю та розсекречуванню за будь-яких обставин не підлягають, доступ до них можуть мати лише керівники та уповноважені ними співробітники відповідного розвідувального органу, насамкінець, відомості про осіб-конфідентів не мають входити до предмету прокурорського нагляду.

Усі вище зазначені моменти можна знайти у Законі РБ «Про органи державної безпеки Республіки Білорусь» та Положенні про Комітет державної безпеки РБ, оскільки основний орган зовнішньої розвідки знаходиться у складі КДБ, але віднести їх напряму до функціональності розвідувальних органів можна лише з великим припущенням.

Висновок: правове регулювання інформаційної безпеки у сфері діяльності розвідувальних органів РБ на даний час знаходиться на початковому етапі. Основні питання діяльності регулюються не на законодавчому рівні, а виключно відомчими закритими нормативно-правовими актами. У найближчому майбутньому слід очікувати прийняття повноцінного закону про зовнішню розвідку, проект якого, за інформацією ЗМІ, декілька разів вже подавався до розгляду у білоруський парламент.

Література

1. Указ Президента Республики Беларусь «О вопросах внешней разведки» от 25 марта 2003 г., № 116 (в ред. Указа Президента Республики Беларусь от 28.05.2008 № 286). URL: // http://pravo.levonevsky.org/.

2. Закон Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах» (в ред. Закона Республики Беларусь от 17.07.2018 № 124-З). URL: http://kgb.by/ru/zakon170-3/.

3. Закон Республики Беларусь от 10 июля 2012 г. № 390-З «Об органах государственной безопасности Республики Беларусь» (в ред. Закона Республики Беларусь от 09.01.2019 № 169-З). URL: // http://www.kgb.by/ru/zakon390-3/.

4. Указ Президента Республики Беларусь от 03.03.1999 № 129 «Перечень сведений, составляющих государственную тайну Республики Беларусь». URL : // http://pravo.levonevsky.org/bazaby11/republic49/text295.htm.

5. Указ Президента Республики Беларусь от 23 июля 2013г. № 325 «Об утверждении Положения о Комитете государственной безопасности Республики Беларусь» URL: // http://www.kgb.by/ru/ukaz325/.

6. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации». URL:http://www.pravo.by/webnpa/text.asp?RN=h10800455.

УДК [34:004]:342.7(477)
Радзієвська О.Г.
кандидат юридичних наук,
старший науковий співробітник,
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

ПРАВОВІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДИТИНИ В УКРАЇНІ

Становлення інформаційного суспільства в Україні та світі нині супроводжується актуалізацією і загостренням інформаційного протистояння на регіональному, державному та міжнародному рівнях. Зміщення акцентів у веденні воєнних конфліктів на комплексне використання воєнних і невоєнних інструментів (економічних, політичних, інформаційно-психологічних тощо) принципово змінює характер трансформаційних процесів у сучасному суспільстві. Спроби несанкціонованого доступу до об'єктів інформаційної інфраструктури України, намагання порушити морально-психологічний стан у суспільстві та дестабілізувати внутрішню соціально-політичну обстановку через застосування цілеспрямованого інформаційного (інформаційно-психологічного) впливу з використанням сучасних інформаційних технологій супроводжуються виникненням новітніх викликів та загроз для людини, суспільства, держави. Загрози інформаційній безпеці людини, суспільства і держави стають все більш небезпечними, а негативний інформаційний вплив на індивідуальну та суспільну свідомість дедалі суттєвішими.

Особливу небезпеку інформаційні загрози становлять для дитини, як суб'єкта суспільних відносин, який потребує особливого захисту і піклування з боку держави та суспільства відповідно до законодавства України і норм міжнародного права. Сучасні трансформаційні процеси в інформаційній сфері суттєво впливають на формування свідомості дитини та її сприйняття навколишнього світу, а інформація негативного змісту здатна викривляти світогляд дитини, підмінювати її морально-етичні цінності, заважати формуванню цілісної та гармонійної особистості. Тому питання захисту інформаційної безпеки дитини в сучасному інформаційному суспільстві у коротко- і довготривалій перспективі буде залишатися вкрай важливою складовою системи забезпечення інформаційної безпеки держави та одним із ключових елементів забезпечення національної безпеки України.

Серед основних пріоритетів забезпечення інформаційної безпеки, відповідно до положень п. 4.11 Стратегії національної безпеки України [1], визнано: забезпечення наступальності заходів політики інформаційної

безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії; протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; розробка і реалізація скоординованої інформаційної політики органів державної влади.

Аналіз сучасного стану забезпечення інформаційної безпеки в Україні дає підстави стверджувати, що система захисту інформаційної безпеки дитини в Україні залишається недостатньо ефективною і такою, що потребує кардинальної трансформації відповідно до сучасних викликів і загроз в інформаційній сфері. Правове забезпечення інформаційної безпеки дитини розвивається фрагментарно, ситуаційно, за відсутності системного підходу та єдиної інформаційної політики держави, що знижує ефективність протидії інформаційним викликам і загрозам та ускладнює організацію превентивних заходів з їх упередження. Як приклад, відсутність єдиної державної інформаційної політики, у тому числі з питань висвітлення ситуації на сході України, монополізація ЗМІ, редакційна політика яких залежить від уподобань їх власників, практично залишає без важелів впливу центральні та місцеві органи виконавчої влади щодо профілактики інформаційних викликів і загроз.

З огляду на зростання рівня небезпек для дитини в інформаційному суспільстві, виникає необхідність використання правового моделювання у правотворчій та правозастосовній практиці, що надасть можливість запобігти дії негативних інформаційних впливів на її свідомість. Розроблення превентивної правової моделі у цій сфері є можливим за умови використання методів правового моделювання розвитку суспільних процесів, що ґрунтуються на всебічному аналізі та прогнозуванні реальних і потенційних загроз інформаційній безпеці людини, суспільства та держави. Для цього необхідним є створення інтегрованої системи оцінки інформаційних загроз, як зазначено в пріоритетних завданнях Стратегії національної безпеки України [1]. Актуальним у цьому питанні видається опрацювання і впровадження в Україні розробленої Європолом системи оцінювання загроз організованої злочинної діяльності в мережі Інтернет (IOCTA). Також доцільно проаналізувати практику держав - членів НАТО у питаннях створення і розвитку інститутів, що відповідають за інформаційно-психологічну безпеку.

При розбудові та забезпеченні функціонування системи захисту прав та безпеки дитини в інформаційному просторі необхідно зважати на те, що згідно із законодавством України відповідальність за її реалізацію лежить не лише на державі та її інституціях, які повинні створювати відповідні умови цієї протидії, але й на кожному громадянинові України, а убезпечення дитини в інформаційному просторі законодавчо покладається

на батьків або осіб, що їх замінюють і на державні органи та інституції, на які покладено функції по охороні дитини. Тому вагомою складовою системи захисту інформаційної безпеки дитини є удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм з інформаційної та медіакультури із залученням громадянського суспільства та бізнесу, про що також йде мова в завданнях Стратегії національної безпеки України [1], та відповідного відображення зазначеного у національному законодавстві.

Література

1. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: указ Президента України від 26.05.2015 № 287/2015. // База даних Законодавство України / ВР України. URL: http://zakon5.rada.gov.ua/laws/show/287/2015.

УДК 355.40

Саричев Ю.О.
кандидат технічних наук,
старший науковий співробітник
Ткаченко В.А.
кандидат військових наук
Зубков В.П.
Національний університет оборони України
ім. Івана Черняховського

ТОПОГЕОДЕЗИЧНА (ГЕОІНФОРМАЦІЙНА) ТА НАВІГАЦІЙНА СКЛАДОВІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ У ВОЄННІЙ СФЕРІ

Державне управління є видом діяльності держави, здійснення управлінського організуючого впливу шляхом використання повноважень виконавчої влади через організацію виконання законів, здійснення управлінських функцій з метою комплексного соціально-економічного та культурного розвитку держави, її окремих територій, а також забезпечення реалізації державної політики у відповідних сферах суспільного життя, створення умов для реалізації громадянами їх прав і свобод.

Необхідність реалізації цілей та завдань державного управління у воєнній сфері зумовлює наявність системи органів державного військового управління, а функції управління розкривають їх сутність та зміст діяльності, співвідношення з іншими органами управління, а також місце в загальній системі управління. Будь-яка функція управління реалізується виключно інформаційним шляхом, тому очевидно, що інформаційне забез-

печення необхідно розглядати як невід'ємну складову системи державного військового управління.

Оскільки ведення бойових дій здійснюється,як правило, на великій території, має комплексний характер застосування військ (сил), озброєння та військової техніки, то неможливо проігнорувати такі види інформаційного забезпечення як топогеодезичне (геоінформаційне) та навігаційне, без яких фактично неможливо здійснювати будь-які дії військ (сил).

Досвід ведення бойових дій на Сході України переконливо показав, що ефективність застосування систем управління військами та зброєю знаходиться в прямій залежності від інформаційного забезпечення, і зокрема від якості навігаційного забезпечення ЗС України, забезпечення геопросторовими даними про місцевість, яка використовується військами (силами).Стрімкий розвиток техніки й технологій забезпечив оснащення ЗС України високотехнологічними та високоточними видами озброєнь, що призвело до зміни характеру ведення бойових дій з подальшим переходом до фактично безконтактної війни з противником.

Загалом, під топогеодезичним забезпеченням ЗС України розуміють комплекс заходів з підготовки та доведення до органів військового управління всіх рівнів та військ топогеодезичних і картографічних даних, топографічних та спеціальних карт (у тому числі електронних), фотодокументів місцевості, а також астрономо-геодезичних, гравіметричних та інших геопросторових даних для здійснення управління військами (силами) та озброєнням в ході виконання ними поставлених задач.

Навігаційне забезпечення це комплекс заходів, які організовуються і здійснюються з метою постійного та об'єктивного отримання в масштабі реального часу військовими об'єктами інформації про власне місцезнаходження для ефективного ведення операцій (бойових дій), застосування озброєння та військової техніки, а також точного і безпечного переміщення наземних, повітряних, надводних та підводних об'єктів військового призначення.

Проведений аналіз свідчить, що сучасні принципи організації топогеодезичного та навігаційного забезпечення у ЗС України впроваджуються недостатньо ефективно, і подальше підвищення бойових можливостей військ неможливе без пошуку нових шляхів інформаційного забезпечення (перш за все, забезпечення геопросторовими даними) військ (сил).

Основними аспектами цього аналізу є:

відповідність обсягу завдань із забезпечення ЗС України засобами навігації, геопросторовими даними реальним фінансовим, матеріальним та інформаційним ресурсам держави;

можливість забезпечення ЗС України навігаційною інформацією та інформацією про місцевість у будь-якому районі;

відповідність існуючих методів і технологій створення, накопичення та використання геопросторових даних реальним потребам військ (сил), у тому числі і на перспективу.

Сучасні вимоги до навігаційного та топогеодезичного забезпечення ЗС України обумовлені необхідністю:

створення, підтримки та удосконалення заданих параметрів локального навігаційного поля для використання ЗС України;

повного оснащення сил та засобів ЗС України засобами навігації;

виконання великих обсягів картографічних робіт при оновленні топографічних карт, що уповільнює процес їх актуалізації;

розвитку інформаційних технологій у сфері топографо-геодезичного та картографічного виробництва, впровадження цифрових методів створення та оновлення картографічних даних;

належного навігаційного забезпечення та забезпечення геопросторовими базами даних ЗС України, створеними у відповідних форматах на єдиній топографічній основі та за єдиними підходами.

Крім того, усталені масштабні ряди топографічних карт сьогодні, як показав досвід ведення бойових дій на Сході України, неповною мірою відповідають потребам ЗС України. Виросли також вимоги до актуальності просторової інформації.

При цьому необхідно враховувати сучасні підходи до картографічного забезпечення держав-членів ЄС та НАТО, міжнародний досвід створення національних інфраструктур геопросторових даних, сучасні тенденції розвитку навігаційних систем, топографо-геодезичної та картографічної діяльності, досвід ведення воєнних дій, конкретні потреби силових структур в засобах навігації, топографо-геодезичній і картографічній інформації в умовах загрози тероризму та кібератак тощо.

Отже, актуальна проблема якісного топогеодезичного та навігаційного забезпечення сил оборони потребує глибокого комплексного наукового дослідження з метою визначення їх ролі і місця в єдиній системі інформаційного забезпечення.

Як складові (види) інформаційного забезпечення топогеодезичне та навігаційне забезпечення мають надавати можливість:

вивчення та оцінки місцевості, орієнтування на ній з визначеною точністю;

виконання вимірювань, розрахунків;

побудови розрахункових моделей ситуацій і процесів, які відбуваються на місцевості.

Таким чином, топогеодезичне та навігаційне забезпечення як невід'ємні складові інформаційного забезпечення державного управління у воєнній сфері потребують подальшого удосконалення з метою якісного виконання комплексу топографо-геодезичних і картографічних робіт та своєчасного задоволення геопросторовими даними потреб ЗС України та інших складових сил оборони.

УДК 355.40: 356.35
Саричев Ю.О.
кандидат технічних наук,
старший науковий співробітник
Хоменко Л.В.
Національний університет оборони України
ім. Івана Черняховського

РОЛЬ ТА МІСЦЕ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ В СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ У ВОЄННІЙ СФЕРІ

Словосполучення “інформаційно-аналітичне забезпечення” досить часто використовується в різних сферах діяльності держави, в тому числі з питань державного управління у воєнній сфері. Аналіз показує, що інформаційно-аналітичне забезпечення в процесі інформаційного забезпечення, зокрема у воєнній сфері, займає особливе місце. Проте сьогодні, на жаль, немає єдиного розуміння цього важливого поняття, в наукових та публіцистичних статтях воно має змістову суперечливість, що породжує проблему, яка пов’язана як з теоретичною недосконалістю цього питання, так і з його практичною реалізацією.

Незважаючи на важливість функції інформаційно-аналітичного забезпечення в процесі інформаційного забезпечення, зокрема у воєнній сфері, на практиці має місце плутанина сутності у використанні зазначеного поняття з іншими взаємопов’язаними (спорідненими) з ним поняттями – “інформаційне”, “довідкове”, “інформаційно-довідкове”, “системний аналіз”, “аналітичне” тощо. На жаль, вільне трактування цього важливого поняття призвело до певної розбіжності не лише на практиці, але і у фахових теоретичних працях. На наш погляд, зазначене є системною методологічною помилкою, яка шкодить реалізації інформаційного забезпечення, зокрема в системі державного управління у воєнній сфері.

Про причини такого незадовільного стану детально висвітлено в роботах [1 – 3]. У цих роботах наведений перелік існуючих визначень інформаційно-аналітичного забезпечення державного управління, а також показано, що багато авторів припускаються методичної помилки, плутаючи складові споріднених функцій двох взаємопов’язаних підпроцесів загального кібернетичного процесу інформаційного забезпечення державного управління – моніторингу та, власне, самого інформаційно-аналітичного забезпечення. Проте в загальному циклі управління необхідно розрізняти окремі функції з їх внутрішніми складовими, що мають конкретне цільове призначення.

Загалом, в інформаційно-аналітичному забезпеченні фахівці виділяють дві складові [4]: а) інформаційну (отримання, систематизація, зберігання і поширення даних (інформації) та б) аналітичну (узагальнення, класифікація інформації, її аналіз і перетворення, розробка пропозицій, рекомендацій та прогнозів)). З теорії інформації відомі такі терміни, як "первинна та вторинна обробка інформації". Очевидно, що первинна обробка інформації здійснюється саме при виконанні функції моніторингу як першого кроку здійснення загального кібернетичного контуру управління (пошук та збір даних), а вторинна обробка є невід'ємною складовою інформаційно-аналітичного забезпечення.

Тому, за аналогією з визначеннями, наведеними в [1, 2], запропоновано наступне визначення: "*інформаційно-аналітичне забезпечення (у воєнній сфері) – комплекс заходів щодо реалізації процесів створення інформаційних продуктів (аналітичних матеріалів) на основі використання статичних інформаційних ресурсів (документованих даних та інформації), отриманих за результатами моніторингу, а також шляхом проведення розрахунків, моделювання ситуацій, аналізу і синтезу даних та інформації, з метою підтримки прийняття рішень органами військового управління всіх рівнів*".

Запропоноване визначення інформаційно-аналітичного забезпечення як виду інформаційного забезпечення в системі державного управління у воєнній сфері відповідає суто конкретній функції у загальному контурі управління, і тому дозволяє більш системно розуміти його роль та місце в цій системі. Роль інформаційно-аналітичного забезпечення полягає у виробленні аналітично обґрунтованих пропозицій щодо прийняття ефективних державних управлінських рішень (на підставі своєчасно отриманих, достовірних та достатніх даних (інформації)), а його місце визначається послідовністю інформаційних процесів у загальному кібернетичному контурі управління, що свідчить про необхідність його реалізації після здійснення завдань моніторингу. Слід погодитися з тим, що в інформаційно-аналітичному забезпеченні одночасно розрізняються дві складові: а) власне інформаційна (отримання, систематизація, зберігання і поширення інформації або даних); б) аналітична (узагальнення, класифікація інформації або даних, їх аналіз і перетворення, розробка пропозицій, рекомендацій та прогнозів).

З метою усунення зазначених системних причин у вищезазначених роботах [1 – 3] наголошується, зокрема, на необхідності чіткого дотримання фундаментального правила щодо реалізації цілісного контуру управління за кібернетичним принципом та чіткого визначення організаційних форм реалізації інформаційного забезпечення на підставі створення належної класифікації його видів.

Література

1. Роль та місце інформаційного забезпечення в системі державного управління / П.М. Сніцаренко, Ю.А. Саричев // Державне управління: теорія та практика (електронне наукове фахове видання НАДУ). – 2016. – № 1. – С.46-56.

2. Теоретичний підхід до інформаційного забезпечення в системі державного управління у воєнній сфері / Ю.О. Саричев // Вісник НАДУ при Президентові України [за заг. ред. Ю.В. Ковбасюка]. – 2016. – № 4 (83). – С.153-160.

3. Інформаційно-аналітичне забезпечення як вид інформаційного забезпечення в системі державного управління / Ю.О. Саричев // Вісник НАДУ при Президентові України [за заг. ред. Ю.В. Ковбасюка]. – 2017. – № 3 (86).

4. Енциклопедія державного управління: у 8 т. / Нац. акад. держ. упр. при Президентові України; наук.-ред. колегія: Ю.В. Ковбасюк (голова) та ін. – К.: НАДУ, 2011. – Т.2: Методологія державного управління / наук.-ред. колегія: Ю.П. Сурмін (співголова), П.І. Надолішній (співголова) та ін. – 2011. – 692 с.

УДК 32.019.51

Селіна М.Б.
кандидат юридичних наук,
Національна академія СБ України

ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАТИВНИХ ТЕХНОЛОГІЙ: БЛАГО АБО ЗАГРОЗИ

Протягом усієї історії людство створювало сприятливі умови для свого існування розробляючи та удосконалюючи засоби праці, комунікації та ін. Сучасний період не є виключенням. Ситуація у світі характеризується стрімким розвитком науки і техніки, значним удосконаленням інформаційно-комунікативних технологій. Проте, такий розвиток, поряд з новими можливостями щодо удосконалення економічних та інших суспільних процесів, несуть і новітні виклики ти загрози, у т.ч. для безпеки держав. Зокрема, нещодавній запуск Китаєм у тестовому режимі найбільшої експериментальної мережі 5G ознаменував початок нової ери розвитку т.зв. «Інтернету речей» та поступової інтеграції мобільної телекомунікації з іншими сферами життя. Так, «Інтернет речей» - це концепція комп'ютерної мережі фізичних речей, які оснащені вбудованими технологіями для взаємодії друг з другом або із зовнішнім середовищем. О.Турчин, директор з розвитку ІТ-бізнесу компанії Ericsson в Україні і Євразії пояснює, що це глобальна мережа підключених до Інтернету речей, оснащених сенсорами, датчиками і засобами передачі інформації. Ці пристрої об'єднані шляхом їх підключення до центрів контролю, управління та обробки інформації. Організація таких мереж розглядається як явище, здатне перебудувати економічні та інші суспільні процеси, шляхом

виключення з частини окремих дій та процесів участь людини, у т.ч. у питанні прийняття окремих рішень. Важливо зауважити, що за даними Ericsson Mobility Report, вже сьогодні у світі нараховується більше 16 млрд підключених пристроїв. До 2022 року – їх число досягне 29 длрд, і 18 млрд з них будуть саме пристроями світу «Інтернета речей». Оптимісти наголошують, що завдяки розвитку «Інтенету речей» значно трансформуються особисті та соціальні аспекти життя суспільства, а також бізнесу і інших різних галузей, а також, що зазначена технологія має потенціал вирішити значне коло глобальних проблем сьогодення, у т.ч. логістичних, медичних та ін. Проте, така технологія несе не лише позитивні зміни, вона привносить і нові ризики та загрози, головним з яких є питання безпеки. На думку багатьох експертів близько 80% пристроїв будуть вразливими ззовні. А отже, можливість зовнішнього впливу на їх роботу у сегменті критичної інфраструктури може призвести до катастрофічних наслідків.

Так, відповідно до звіту Національної розвідувальної ради США «Інтернет речей» фігурує як одна з шести підривних технологій, зокрема наголошується, що розповсюдження та непомітне для людей перетворення в Інтернет вузли таких речей, як побутова техніка, меблі, паперові документи тощо, можуть значно підвищити ризики у сфері національної інформаційної безпеки.

Значні недоліки та загрози щодо використання «Інтеренету речей» продемонстрував дослідник Цезар Керрудо, який довів, що може «зламати» систему керування руху транспорту і змінити напрям транспортного потоку. Він пояснив, що, у своєму експерименті, він зміг це зробити за допомогою найпростішого програмного забезпечення, шляхом «зараження» датчиків руху транспорту. Ц. Керрудо зазначив, що, враховуючи стрімкий розвиток, зокрема «розумних міст», які вже незабаром можуть бути повністю підключені до глобальної мережі, у разі відсутності належного рівня захисту від зовнішнього втручання у процес їх управління та функціонування, зловмисники та терористи можуть отримати контроль над такими містами, у т.ч. для дестабілізації ситуації в них, організації терористичних атак на політичних та громадських діячів, вчинення масштабних терористичних актів тощо.

Крім цього, недостатня увага щодо ризиків, які тягне за собою «Інтернет речей», створює передумови до і витоку інформації. Сьогодні значне коло т.зв. «розумних речей» можуть збирати, накопичувати та передавати інформацію. Об’єм даних, що збираються, їх вид (аудіо, відео та ін.) залежить від типу пристрою, а спосіб їх передачі та зберігання, залежить від «бажання» їх розробників та виробників.

Отже, «Інтернет речей», поруч із благами для суспільства, привносить і нові виклики і загрози для його стабільного розвитку і функціонування, у т.ч. терористичного характеру. Так, можливість зовнішнього впливу на процес управління пристроїв, об’єднаних з глобальною мережею, створює передумови як для незначної дестабілізації роботи окремих підприємств,

так і для скоєння масштабних терористичних атак, у т.ч. на об'єктах критичної інфраструктури.

Зважаючи на зазначене, приділення належної уваги до забезпечення високого рівня інформаційної безпеки держави не лише не втрачає своєї актуальності, а потребує постійного розвитку та удосконалення цього рівня у відповідності до рівня розвитку та удосконалення інформаційно-комунікативних технологій.

Література

1. Disruptive Civil Technologies. Six Technologies with Potential Impacts on US Interest out to 2025. National Intelligence Council (11 April 2008).

2. Власюк О.С. Національна безпека України: еволюція проблем внутрішньої політики : Вибр. наук.праці/ О.С.Власюк. – К.: НІСД, 2016. – 528 с.

3. Скуратовский Б. Глава британской спецслужбы считает, что появление технологии 5G усилит угрозу кибертерроризма [Електронний ресурс] / Борис Скуратовский // MEDIASAT – Режим доступу до ресурсу: https://libking.ru/books/nonf-/nonf-publicism/190336-edvard-berneys-propaganda.html.

4. Что такоє Интернет вещей и зачем он нужен? [Електронний ресурс] // Новое время – Режим доступу до ресурсу: techno.nv.ua.popscience.

УДК 353

Ситник С.С.
Столяренко В.М.
Національна академія Служби безпеки України

РОЛЬ КОМУНІКАЦІЇ У ДІЯЛЬНОСТІ КЕРІВНИКА ОРГАНУ (ПІДРОЗДІЛУ) СБ УКРАЇНИ

Ускладнення оперативної обстановки за усіма напрямами службової діяльності Служби безпеки України, виникнення нових загроз національній безпеці для нашої країни, зумовлених, насамперед, анексією Російською Федерацією Криму, а також збройним протистоянням на Сході України, вимагають постійного удосконалення службової діяльності органів і підрозділів СБ України, що зокрема передбачає підвищення ролі керівника у розв'язанні складних завдань у сфері забезпечення державної безпеки.

Вирішення цього завдання можливе лише за умов формування керівника як професіонала нової генерації, здатного адекватно реагувати на існуючи виклики та загрози національній безпеці у сучасних умовах, продукувати нові підходи та ідеї щодо організації оперативно-службової діяльності і спроможного використовувати інноваційні технології налагодження взаємин (діалогу) та ділового спілкування з керівниками різних рівнів управління, підлеглими та громадськістю в інтересах вирішення завдань, визначених для органу (підрозділу) СБ України.

Сучасна управлінська діяльність керівника Служби має свої специфічні ознаки, оскільки часто вона відбувається в екстремальних умовах. При

цьому керівнику доводиться відповідати за дії кожного підлеглого, а не лише за свої особисті вчинки. За таких умов надзвичайно важливу роль відіграє рівень комунікативного розвитку керівника, його вміння використати та розкрити свій внутрішній потенціал у певній ситуації.

Накопичений в СБ України досвід організації службової діяльності свідчить про те, що у багатьох типових ситуаціях, які ускладнювали оперативну обстановку на території оперативної відповідальності органу чи підрозділу, узяти її під контроль та локалізувати можливі негативні наслідки вдається лише завдяки високим професійним якостям керівників різного управлінського рівня та їх високо розвиненому комунікативному потенціалу.

Комунікація у сфері управління службовою діяльністю в СБ України – це процес обміну інформацією, який включає в себе отримання керівником первинної інформації, її аналіз, прогноз та передачу підлеглим, але вже у формі завдань на основі прийнятих управлінських рішень, посадовим особам вищого рівня - у формі доповіді, взаємодіючим органам (підрозділам) - у вигляді різного роду орієнтувань.

Будь-який керівник здійснює комунікацію протягом усього робочого дня: і коли розмовляє по телефону, і коли проводить службову нараду, співбесіду, бере участь у робочих зустрічах з взаємодіючими суб'єктами, і коли розв'язує конфліктні ситуації у колективі та таке інше.

Успіх управлінської діяльності багато у чому залежить від уміння керівника налагодити дієву систему комунікації. Тому сучасний керівник має володіти знаннями та здібностями, яким раніше достатня увага не приділялася. З огляду на це у ході підготовки сучасних керівників у першу чергу на відповідних потоках підвищення кваліфікації НА СБ України дуже важливо приділяти належну увагу розвиненню у них перш за все комунікативних знань та умінь, а також здатності ефективно застосовувати їх у повсякденній роботі з організації процесу управління органом (підрозділом) СБ України.

Комунікація повинна допомогти керівнику реалізовувати такі основні функції управління як дослідження оперативної обстановки на території оперативної відповідальності і прогноз її розвитку, прийняття рішення в інтересах своєчасного реагуванню на існуючи виклики та загрози з метою попередження (недопущення) настання негативних наслідків, планування,мотивація, обмін інформацією між взаємодіючими підрозділами, контроль тощо.

Уміле застосування керівником навичок комунікації сприятиме також ефективному виконанню пріоритетних й функціональних завдань та досягненню підрозділом кінцевих результатів за основними напрямами службової діяльності,формуванню здорового морально-психологічного клімату у колективі і розвитку творчих здібностей особового складу, встановленню та підтриманню на належному рівні ділових стосунків з представниками місцевих органів влади та управління, підприємств, організацій тощо.

Водночас,досвід сучасної службової діяльності органів та підрозділів СБ України свідчить про те, що розвиток комунікативного потенціалу теперішніх керівників інколи перебуває на низькому рівні, що спонукає окремих із них до обрання авторитарного стилю керівництва особовим складом. Такі керівники як правило не цікавляться підлеглими, не враховують їх психологічні особливості, емоційний стан, особисті та ділові якості. Рішення такими керівниками, здебільшого, приймаються одноосібно, що не сприяє гуртуванню колективу, формуванню команди однодумців, професійному зростанню підлеглих, їх мотивації до виконання завдань із забезпечення державної безпеки на доручених ділянках роботи. Зазначений підхід до організації процесу управління підлеглими в умовах просування України у напрямку побудови нового суспільства з європейськими цінностями є вкрай неприйнятним та шкідливим.

Тому кожен сучасний керівник повинен мати не тільки фахові навички та уміння, а й зобов'язаний мати якості, що характеризують наявність у нього високо розвиненого комунікативного потенціалу, і у першу чергу уміння працювати з людьми, бути здатним застосовувати більш прогресивні стилі управління, що базуються на повазі до людини та її особистості.

Література

1. Бацевич Ф.С. Словник термінів міжкультурної комунікації. - К.: Довіра,2007. - 205 с.

2. Головне управління державної служби України: методичнірекомендації щодо побудови механізму оцінки ділових і професійних якостейдержавних службовців. - К., 2006. - 8 с.; Рекомендації до визначеннякомпетентностей державних службовців. - К., 2006.

3. Закон України "Про основні засади розбудови інформаційногосуспільства в Україні на 2007-2015 роки" від 9 січня 2007 р. // [Електроннийресурс]. - Режим доступу : www.rada.gov.ua.

УДК 355.40

Сніцаренко П.М.
доктор технічних наук,
старший науковий співробітник,
Національний університет оборони України
імені Івана Черняховського

ЗАКОНОДАВЧІ АКСІОМИ ТА ЇХ ВПЛИВ НА ТЕОРІЮ І ПРАКТИКУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Словникові джерела свідчать, що аксіомою вважається незаперечне твердження, яке не потребує доведення, але служить підставою для доведення інших тверджень. Для суспільного життя, суспільних наук та дер-

жавної діяльності окремої країни аксіоматичним базисом є національна конституція та державні закони, положення яких мають значення окремих аксіом за певними напрямами упродовж деякого періоду аж до внесення відповідних конституційних або законодавчих змін.

Щодо інформаційної безпеки України слід зазначити, що у цьому випадку фундаментальним слід вважати положення статті 17 Конституції України, де визначено, що *забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього Українського народу*. Зауважимо, що зазначена вимога ставиться в один рівень із захистом суверенітету і територіальної цілісності України та забезпеченням економічної безпеки держави, що означає найвищий державний пріоритет діяльності за цим напрямом. Причому про інше стосовно інформаційної сфери в Конституції України не йдеться. Тому позначимо це положення для інформаційної сфери України як **аксіома 1**.

Наслідок з аксіоми 1. Оскільки в Конституції України, крім статті 17, пряме посилання стосовно інформаційної сфери відсутнє, тому *сутність державної інформаційної політики має бути спрямована на забезпечення інформаційної безпеки держави* з відповідним наступним законодавчим роз'ясненням і деталізацією.

На жаль, цього не сталося, тому що поняття *"державна інформаційна політика"* не визначене жодним законодавчим актом України з рядом негативних наслідків як для теорії цього напряму діяльності, так і для практики.

Проведений аналіз показує, що, незважаючи на досить велику кількість сучасних публікацій вітчизняних фахівців на тему інформаційної безпеки або інформаційної політики, концептуального підходу, який би виходив із вищенаведеної конституційної норми, в існуючих теоретичних напрацюваннях поки-що немає. Тому до сьогодні залишається невирішеною задача розробки не те що теорії, але навіть теоретичних основ забезпечення інформаційної безпеки України, що особливо шкодить законодавчій та нормотворчій практиці. Із-за цього в чинному законодавстві України існує неоднозначність у формулюванні сутності одних і тих же термінів, понять і положень, наслідком чого практична діяльність дезорієнтується, що призводить до подальшого довільного розуміння та використання термінів, понять і положень, їх ситуативної модифікації, ігнорування у випадках, коли таке недоцільне. Це, відповідно, призвело до труднощів системного характеру, пов'язаних із неузгодженістю на загальнодержавному рівні позицій різних зацікавлених сторін, що не дозволило сформувати та запровадити в Україні єдину та чітку державну інформаційну політику і механізми її реалізації, спрямованих якраз на забезпечення інформаційної безпеки держави.

Зазначене гальмує загальний процес створення в Україні повноцінної системи забезпечення інформаційної безпеки держави та не дозволяє в сучасних динамічних умовах протікання інформаційних процесів найбільш раціонально втілювати в життя практичні заходи. Такий стан спричиняє

актуальну науково-практичну проблему, яка полягає в *неможливості створення в Україні повноцінної та ефективної системи забезпечення інформаційної безпеки держави із-за недосконалого національного інформаційного законодавства та відсутності відповідної системної теоретичної бази.* Це потребує пошуку шляхів її розв'язання, у першу чергу, на теоретичному рівні.

Становлення теоретичних основ забезпечення інформаційної безпеки України, виходячи із принципу системного підходу, має ґрунтуватися на вищенаведеній *аксіомі 1*, а також на інших аксіомах, що містяться у чинному законодавстві держави. Розглянемо таку можливість.

Зокрема, на основі аксіоми 1 може бути визначена сутність державної інформаційної політики України у такій редакції:

державна інформаційна політика України – складова державної політики як сукупність політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових та організаційних завдань і заходів, *спрямованих на забезпечення інформаційної безпеки України.*

Надалі для теоретичної бази, формування та реалізації цієї політики першочергово потрібне чітке законодавче розуміння (тлумачення) сутності інформаційної безпеки держави. Незважаючи на те, що в законодавчому полі України все ще відсутній рамковий закон про інформаційну безпеку держави, законодавство визначило сутність інформаційної безпеки в "тілі" нерамкового Закону України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" [1]. У законодавчих актах України, які стосуються інформаційної сфери та набрали чинності після цього закону, інше тлумачення інформаційної безпеки або його заперечення чи уточнення відсутні. Тому, попри деякі незначні недоречності цього визначення, його можна сприймати як наступну законодавчу аксіому для інформаційної сфери України, яка далі подається в редакції названого закону.

Аксіома 2. "*Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:*

неповноту, невчасність та невірогідність інформації, що використовується;

негативний інформаційний вплив;

негативні наслідки застосування інформаційних технологій;

несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації".

Ця законодавча аксіома не суперечить фундаментальній аксіомі 1, деталізуючи її, та відповідає принципу системного підходу. Таке законодавче формулювання сутності інформаційної безпеки може бути уточнене (принаймні, шкоду наносить як "*невчасність*" інформації, так і "*відсутність*" інформації, тобто неможливість її отримання за нагальної потре-

би), але загалом воно є достатньо чітким предметно, узагальненим та системно збалансованим.

Наслідок 1 із аксіоми 2. *Кібернетична безпека (кібербезпека) – інформаційна безпека в просторі електронних інформаційних ресурсів.* Тому штучне (адміністративне) роз'єднання інформаційної безпеки та кібербезпеки суперечить логіці протікання інформаційних процесів, порушує принцип системності, отже є недопустимим і для теорії, і для практики. Але в чинній Стратегії національної безпеки України [2] таку помилку допущено, що має негативні наслідки для інформаційного законодавства України, а тому і для подальшого викривлення теорії та спотворення практики.

Наслідок 2 із аксіоми 2. Очевидними стають *загрози інформаційній безпеці України* (незалежно від джерела їх походження – агресія, непрофесійна діяльність, неспроможність, злочинна бездіяльність), котрі, матеріалізуючись на практиці, *можуть нанести шкоду* людині, суспільству чи державі:

неповнота, невчасність та невірогідність інформації, що використовується, які спричиняються обмеженими функціональними можливостями національної інформаційної інфраструктури, елементи якої формують інформаційний (у тому числі кібернетичний) простір держави;

негативний інформаційний вплив, а також *негативні наслідки застосування інформаційних технологій*, що спричиняються цілеспрямованими діями елементів ворожої інформаційної інфраструктури або навмисними чи ненавмисними діями елементів національної інформаційної інфраструктури, які формують інформаційний простір держави;

несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, що може статися із-за недосконалості систем безпеки (захисту) інформації на. елементах національної інформаційної інфраструктури, які формують інформаційний простір держави.

Зауважимо, що у Стратегії національної безпеки України наведено інше – пунктом 3.6. визначено такі загрози інформаційній безпеці: *ведення інформаційної війни проти України; відсутність комунікативної політики держави; недостатній рівень медіакультури суспільства,* що не відповідає вищенаведеному законодавчому визначенню сутності інформаційної безпеки, тобто аксіомі 2 та об'єктивному наслідку 2 із неї, маючи при цьому більш політичне, ніж власне інформаційне, забарвлення. Зазначений стратегічний, але несистемний наратив, зокрема, відчутно поширився на чинну Доктрину інформаційної безпеки України [3], яка із-за цього не може вважатися самодостатньою.

Наслідок 3 із аксіоми 2. *Забезпечення інформаційної безпеки України* (в тому числі у кіберпросторі) також є цілком очевидним і полягає в реалізації запобіжних заходів проти нанесення шкоди із-за:

неповноти, невчасності та невірогідності інформації, що використовується;

негативного інформаційного впливу;

негативних наслідків застосування інформаційних технологій;

несанкціонованого розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

На стратегічне спрямування таких запобіжних заходів вказано у цьому ж Законі України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки", де визначено шлях вирішення проблеми інформаційної безпеки. Ґрунтуючись на цьому положенні, майже дослівно запишемо наступну законодавчу аксіому.

Аксіома 3. *Шляхом забезпечення інформаційної безпеки України (вирішення проблеми інформаційної безпеки) має бути:*

створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері.

На наш погляд, наведені законодавчі аксіоми та очевидні наслідки із них мають закласти певну фундаментальність у будь-яку діяльність, що спрямована на забезпечення інформаційної безпеки України, у першу чергу, в процес обґрунтування та становлення теоретичних основ цієї найпріоритетнішої галузі діяльності як запоруки проведення адекватних практичних заходів та створення ефективної загальнодержавної системи.

Література

1. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" від 09.01.2007 р. № 537-V // Законодавство України [Електронний ресурс]. – Режим доступу: http: // zakon3.rada.gov.ua. (дата звернення 25.02.2019).

2. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 р. № 287/2015 [Електронний ресурс]. – Режим доступу: http: // zakon5.rada.gov.ua. (дата звернення 25.02.2019).

3. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25.02.2017 р. № 47/2017 [Електронний ресурс]. – Режим доступу: http: // president.gov.ua. (дата звернення 25.02.2019).

УДК 343.341
Остроухов В.В.
доктор філософських наук, професор
Присяжнюк М.М.
кандидат технічних наук,
старший науковий співробітник,
Національна академія Служби безпеки України

ТЕРОРИЗМ В АСПЕКТІ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

Тероризм (англ. terrorism) – суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей [1].

Протягом всієї історії свого існування людство стикалося з різними формами та проявами тероризму. Саме в перехідні етапи життя суспільства тероризм має тенденцію росту і набуває особливої гостроти в період соціальних конфліктів.

Аналіз наукової літератури показує, що сучасному тероризму властиві чотири характерні ознаки:

- використання крайніх форм насильства або погроза таким насильством;
- вихід терористичного акту за межі завданого цілям руйнування, заподіяння тілесних ушкоджень, смерті;
- досягнення цілі терористичного акту шляхом психологічного впливу на осіб, які не є безпосередніми жертвами насильства;.
- вибір жертв тероризму більше за їх символічним, чим дійсним значенням [2].

Сучасний тероризм розглядають як спосіб інформаційно-психологічного впливу з метою управління соціумом через превентивне залякування та досягнення соціально-політичних і економічних цілей.

За своєю суттю тероризм – явище, засноване на використанні інформаційно-психологічних технологій, здатних масово викликати віртуальний страх. Його часто ототожнюють з поняттям «терор».

Однак тероризм має ряд характерних ознак, відмінних від терору.

По-перше, тероризм – це одноразовий акт або серія аналогічних актів, а терор носить тотальний, масовий, безперервний характер.

По-друге, суб'єкти тероризму, на відміну від суб'єктів терору, ніяких офіційно встановлених владних повноважень не мають.

По-третє, суб'єкти терору – це суспільно-політичні структури, які мають необмежену владу над населенням, а суб'єкти тероризму – фізичні осудні особи, які досягли віку кримінальної відповідальності.

По-четверте, суб'єкти терору здійснюють залякування населення з

метою його спонукання до певної поведінки, тоді як суб'єкти тероризму здійснюють залякування населення з метою спонукання до певної поведінки влади, міжнародної організації, фізичної чи юридичної особи або групи осіб.

По-п'яте, терор – це соціально-політичний фактор реальності, а тероризм – кримінально-злочинна дія [3].

Синонімами для поняття «терор» є «політика терору», «масовий терор», «тотальний терор». Синонімами для поняття «тероризм» є «терористичний акт», «злочин терористичної спрямованості», «терористичний злочин», «терористична діяльність».

Терористична діяльність є складною, ієрархічно побудованою, багатофункціональною й динамічною системою, яка має свою зовнішню психологічну структуру. Психологічний аналіз діяльності передбачає виділення в ній основних структурних компонентів і встановлення характеру зв'язку між ними. До них відноситься мотив, мета, дії, способи, умови, операції, засоби, результат діяльності і зворотний зв'язок.

Сучасний тероризм враховує особливості інформаційної епохи, пов'язаної з існуванням глобальних ЗМІ, готових оперативно висвітлювати «терористичні сенсації» і здатних за допомогою певних коментарів до подій ефективно впливати на громадську думку в будь-якій країні світу. В епоху інформаційного буму, здатність доносити будь-які відомості до мільярдів людей за секунди робить ЗМІ унікальними механізмами інформаційно-психологічного впливу на населення. Цей вплив стає ще більш масованим, глибоким і ефективним, якщо ЗМІ знаходяться «в руках» професіоналів, які володіють пером і словом, вміло поєднують в процесі контакту зі своєю аудиторією раціональну та емоційну складові представленої інформації. У цій ситуації остання сприймається не тільки на рівні свідомості, а й на більш тонкому, глибинному, психологічному підсвідомому рівні, що гарантує більш повне її засвоєння і тривалий вплив на вчинки людини [4].

Боротьба з сучасним тероризмом має бути насамперед націлена на створення системи знань, навичок та умінь у протидії цьому явищу. А знання інформаційно-психологічних аспектів тероризму дозволить своєчасно виявляти терористичні загрози, визначати та аналізувати причини їх виникнення, з'ясовувати проблеми, сутність і тенденції тероризму, прогнозувати, попереджати та присікати терористичні акти.

Література

1. Закон України «Про боротьбу з тероризмом» від 20.03.2003 № 638-IV // Відомості Верховної Ради України. – 2003. – № 25. – Ст. 180.

2. Современный политический экстремизм: понятие, истоки, причины, идеология, проблемы, организация, практика, профилактика и противодействие. Рук. авт. колл. Дибирова Н. З., Сафаралиев Г. К. Махачкала. 2009. 640 с.

3. Терроризм: определения и сущность: монографія / [А. В. Коростыленко, Б. Д. Леонов, И. Н Рыжов и др.] ; под. общ. ред.. В. В. Крутова, И. И. Мусиенко, В. А. Глушкова. – К.: Центр уч.-науч. и науч.-практ. изданий НА СБ Украины, 2014. – 192 с.

4. Электронные СМИ и терроризм / И. Панарин – 04.01.2019 [Електронний ресурс] – Режим доступу: panarin.com/smi/80-smi-i-terrorizm.html.

УДК 341.824:338.47 (043.2)

Тиква В. Л.
Національна академія Служби безпеки України

ОКРЕМІ ПРАВОВІ ПРОБЛЕМИ ПРОТИДІЇ РОЗПОВСЮДЖЕННЮ ДЕСТРУКТИВНИХ МАТЕРІАЛІВ У МЕРЕЖІ ІНТЕРНЕТ В УКРАЇНІ

Останніми роками інтенсивність та обсяг розповсюдженої інформації значно перевищують природні можливості людини для її опрацювання. Значна частина суспільства в силу різних суб'єктивних та об'єктивних обставин не схильна до критичного осмислення отриманих даних. Це дозволяє різним суб'єктам формувати деструктивні інформаційні потоки та використовувати їх з метою неправомірного впливу на свідомість і поведінку інших людей. Особливо гостро ця проблема відчутна у мережі Інтернет, так як вона надає можливість необмеженому колу осіб практично безвідповідально створювати, обробляти, поширювати та зберігати значні масиви інформаційних даних. Анонімність, вільний, дешевий та екстериторіальний доступ у режимі реального часу до інформації зробили Інтернет зручним союзником правопорушників.

У силу своєї природи Інтернет є віртуальним середовищем, однак все що в ньому відбувається має реальний вплив на процеси реалізації прав, свобод та інтересів людини, суспільства і держави. На сьогодні життя соціуму розділилося на дві частини: реальну і віртуальну. В реальному житті поведінка людини визначається різними соціальними нормами, а у віртуальному – фактично не існує універсальних правил гри, кожен діє на свій розсуд і відповідно до своїх принципів та цінностей. Усі намагання світової спільноти чи окремих держав запровадити всебічне правове регулювання цього середовища поки що були малорезультативними.

Відсутність правових засобів регламентації та контролю за змістом інформації, яка циркулює в Інтернеті, дозволяє багатьом розгорнути у цій мережі активну інформаційну діяльність, зокрема екстремістського спрямування. Екстремісти одинаки, екстремістські організації та інші зацікавлені особи розповсюджують в Інтернеті відомості, які прямо чи опосередковано спрямовані на навіювання або розпалювання екстремістських настроїв у населення, зокрема і нашої держави.

В Інтернеті створена та функціонує велика кількість інформаційних ресурсів (сайтів), які сприяють розвитку екстремізму. На думку фахівців, такі сайти умовно можна розділити на чотири основні групи, а саме: 1) сайти, які безпосередньо поширюють деструктивні ідеї, підбурюють сепаратистські та терористичні настрої; 2) інформаційні ресурси, що здійснюють медійну підтримку представників міжнародних екстремістських та терористичних організацій; 3) сайти, що розпалюють ксенофобію на основі расової чи національної приналежності; 4) інформаційні ресурси довідкового характеру, які побічно закликають до протиправної діяльності [1].

В окремих випадках розповсюдження в мережі деструктивних матеріалів різного спрямування є одним із способів ведення кібервійни. Такі елементи інформаційного протиборства як розміщення в Інтернеті завідомо неправдивої або провокаційної інформації, маніпулювання суспільною свідомістю, нав'язування ідеології нетерпіння користувачам, підрив міжнародного авторитету держави, створення атмосфери бездуховності і аморальності, негативного ставлення до культурної спадщини, дестабілізація політичних відносин в суспільстві, поширення компромату та інших відомостей, що ганьблять честь і гідність політичної еліти країни, підбурення суперечок між партіями, громадськими об'єднаннями та рухами, розпалювання міжнаціональної ворожнечі та расової нетерпимості, ініціювання масових заворушень й інших протестних акцій тощо [2, с. 39] можуть використовуватися певними екстремістами та їх організаціями не тільки у власних цілях, але й також на користь конкретних держав. При цьому вказана екстремістська діяльність, як правило, контролюється й супроводжується іноземними спецслужбами, що лише ускладнює процеси протидії та ліквідації її негативних наслідків.

В епоху цифрових технологій деструктивна діяльність вийшла на якісно новий рівень функціонування. Екстремісти мають змогу розміщувати відповідні матеріали на серверах, які фізично знаходяться на території інших держав. У зв'язку з цим в органах державної влади України відсутні повноваження на втручання у їхню роботу з метою недопущення поширення шкідливої інформації.

Ми вважаємо, що розповсюдження в Інтернеті деструктивних матеріалів становить загрозу національним інтересам України, оскільки здатне спровокувати значні соціальні конфлікти в економічній, політичній, релігійній та інших сферах суспільного життя, а також посягнути на конституційний лад, територіальну цілісність і незалежність держави.

В Україні на конституційному рівні кожному гарантовані права на свободу думки і слова, на вільне вираження своїх поглядів і переконань, на вільне збирання, зберігання, використання і поширення інформації усно, письмово або в інший спосіб – на свій вибір. Здійснення цих прав може бути обмежене законом, зокрема, в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання за-

ворушенням чи злочинам, для захисту репутації або прав інших людей, для підтримання авторитету і неупередженості правосуддя (стаття 34 Основного Закону України) [3]. Незважаючи на те, що українське законодавство встановлює відповідні обмеження та юридичну відповідальність за окремі види інформаційної діяльності, однак вони є малоефективними під час протидії деструктивній діяльності в Інтернеті. Особливо це стосується боротьби з поширенням у цій мережі агітаційно-пропагандистських матеріалів, які екстремісти використовують заради впливу на свідомість громадян.

Так, чинний Кримінальний кодекс України передбачає кримінальну відповідальність за насильницьку зміну чи повалення конституційного ладу (ст. 109), посягання на територіальну цілісність і недоторканість України (ст. 110), порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками (ст. 161), заклики до вчинення дій, що загрожують громадському порядку (ст. 295). Проте, як наголошує Н. Савінова, у ньому не криміналізовані інформаційно-психологічні впливи на свідомість людей із цією метою. Вона вважає, що саме шляхом здійснення впливу на свідомість можливе втягнення населення у вчинення подібних злочинів, зокрема – утягнення в сепаратистські рухи, екстремістські організації та релігійні секти [4, с. 192]. Оскільки такі впливи здійснюються, зокрема, і через Інтернет ресурси, то очевидною є необхідність вдосконалення кримінального законодавства у цій сфері.

На нашу думку, вироблення правових механізмів протидії розповсюдженню деструктивних матеріалів у мережі Інтернет має відбуватися у комплексі з іншими заходами, спрямованими на вдосконалення правового регулювання Інтернет-відносин. В Україні держава і суспільство мають досягнути згоди щодо допустимих меж втручання у свободу інформаційної діяльності людини, адже за відсутності розумних та справедливих обмежень, які відповідають сучасним викликам та загрозам, поступальний демократичний розвиток соціуму практично не можливий.

Література

1. Костихин А. А. Интернет как инструмент террористических и экстремистских организаций в психологической войне [Електронний ресурс] / А. А. Костихин. – Режим доступа : http://www.iimes.ru/?p=4737.

2. Акопов Г. Л. Глобальные проблемы и опасности сетевой политики : монография / Г. Л. Акопов. – Ростов-на-Дону : ООО «Ростиздат», 2004. – 128 с.

3. Конституція України : Закон України від 28 червня 1996 р. № 254к/96–ВР / [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/254 %D0 % BA/96-%D0 %B2 %D1 %80.

4. Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні : теоретичні та практичні аспекти : монографія / Н. А. Савінова. – К. : ДКС, 2011. – 342 с.

УДК 351.862.4
Устименко О.В.
кандидат наук з державного управління,
старший науковий співробітник,
Національний університет оборони України
ім. Івана Черняховського

ПЕРСПЕКТИВНА СИСТЕМА МОНІТОРИНГУ ТА АНАЛІЗУ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ МІНОБОРОНИ РФ

Намір отримати в своє розпорядження систему моніторингу та аналізу інформації з відкритих джерел Міноборони Росії вперше озвучило в 2015 році. Роботи зі створення даної системи знаходилися в руслі завдань, що стояли перед створеним у грудні 2014 року Національним центром управління обороною (далі НЦУО).

Основу НЦУО складають три центри управління, два з яких проводять моніторинг обстановки як усередині країни, так і за кордоном, що в обов'язковому порядку передбачає роботу з відкритими джерелами. При цьому за сформованої ще в першій половині XX століття практики, «моніторинг військово-політичної обстановки в світі» багато в чому ґрунтується саме на «читанні газет» і вивченні іншої легальної інформації.

Для вирішення вище окреслених завдань на порталі держзакупівель МО РФ було розміщено заявку з ціною контракту в 30 мільйонів рублів на закупівлю ліцензій на використання системи моніторингу та аналізу ЗМІ. Зі змісту даної заявки було видно основні вимоги до системи аналізу відкритих джерел. Коротко вони такі: система повинна обробляти не менше 20 тисяч відкритих джерел; інформація повинна групуватися по заданим темам; система повинна бути розрахована на 150 користувачів.

Під час закупівель були сформульовані наступні вимоги до системи – її використання повинно істотно підвищити оперативність доведення інформації до керівного складу Міноборони РФ про суттєві події, пов'язані з діяльністю військового відомства, і реакції громадянського суспільства на них за рахунок впровадження нових високотехнологічних рішень, що забезпечують безперервний автоматизований моніторинг ЗМІ, а також аналіз даних на основі статистичних та лінгвістичних технологій».

У січні 2015 року стало відомо, що холдингом «Системи управління» буде створюватися програмно-апаратний комплекс аналізу військово-політичної обстановки, суспільно-політичної, а також соціально - економічної ситуації в країні. Комплекси призначені для оперативного спостереження через відкриті джерела – ЗМІ та соціальні мережі – за політичною, економічною, суспільною ситуацією навколо РФ і всередині країни,

за суспільними настроями і реакціями на різні події, проблемами що назрівають в суспільстві та економіці.

За словами генерального директора холдингу «Системи управління» створювана система буде здатна: відбирати в потоці інформації світових ЗМІ ті повідомлення, які відносяться до заданого запиту; аналізувати не тільки друкований текст і цифрове телебачення, але і ефірне мовлення, працюючи з матеріалами прямого ефіру, якісно автоматично переводячи мову в текст; розпізнавати зображення і ідентифікувати людей та об'єкти; аналізувати частоту висловлювань по тематиці, їх оцінку в соціальних мережах; збирати інформацію, складати і обробляти запит на логічний і смисловий пошуки; моделювати сценарії розвитку обстановки; готувати пропозиції керівництву в автоматизованому режимі. Для вирішення поставлених завдань, за словами розробника, були запропоновані власні алгоритми автоматичного збору інформації, її обробки і класифікації, а також моделі експертної оцінки і можливих варіантів розвитку. Підсумковий інформаційний продукт система повинна формувати з інформаційних блоків в багаторівневому вигляді. Верхній рівень містить підсумкову аналітику, загальні висновки про ситуацію, щодо якої надійшов запит, аналіз звітів і вибір варіантів вирішення проблем. Середній рівень – більш детальна інформація, що включає діаграми, графіки, формування звітів, прогнозування розвитку ситуації. На нижчому рівні можна простежити періодичність, частоту і швидкість оновлення інформації, місце формування події або ситуації аж до конкретного повідомлення, яке увійшло в статистику, переглянути потрібний файл, телесюжет або текст повідомлення в ЗМІ. Декларувалося, що за допомогою системи наочно можна буде побачити тенденції зміни обстановки в конкретних регіонах країни і світу.

Втім ефективність програмно-апаратного комплексу, який може пропонувати керівництву варіанти дій, викликає сумніви. По перше, у відкриті джерела потрапляє багато фейкової інформації, яку комп'ютерна система правильно розпізнати не в змозі. По друге – відображення реальності у відкритих джерелах навмисно спотворюється в політичних, економічних та інших цілях, що може негативно позначитися і на якості комп'ютерного аналізу. Крім того необхідно враховувати, що апаратна частина містить імпортні комплектуючі та неминуче доведеться звертатися до розробників програмного забезпечення, на якому побудована мережа Інтернет, що створює загрозу зовнішнього втручання в роботу аналітичної системи МО РФ.

Дослідження вітчизняних експертів свідчать, що зазначені сумніви не безпідставні. Якщо аналізувати інформацію в Інтернеті то можна прийти до висновку, що вона поширюється як за допомогою великих онлайнових ЗМІ та соцмереж, так і з допомогою розгалуженої системи «помийних» сайтів, новини на яких часто дуже низької якості або навіть повністю вигадані. При цьому вони збирають понад 50 мільйонів візитів на місяць.

Для порівняння, «Українська правда» збирає лише 15 мільйонів візитів на місяць.

Для усунення ризиків неминуче доведеться використовувати ланку аналітиків високої кваліфікації, які будуть фільтрувати і інтерпретувати отриману від систему інформацію. Але в цьому випадку враження від грандіозності і просунутості системи миттєво випаровуються, тому що вона стає просто ще одним допоміжним засобом отримання і обробки даних в роботі з інформацією – відповідальність за висновки цілком лягає на штат аналітиків.

Дізнатися реальні можливості системи можна було б після її впровадження. Закінчення робіт було заплановано на середину 2016 року. Однак ні в зазначений термін, ні в подальшому інформація про створення системи моніторингу відкритих джерел в МО в пресу не потрапляла.

УДК 342.5(477)

Форноляк В.М.
кандидат психологічних наук,
Національна академія Служби безпеки України

ЩОДО ІНФОРМАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ВЗАЄМОДІЇ СУБ'ЄКТІВ БОРОТЬБИ З ТЕРОРИЗМОМ

Перед Україною в даний час досить гостро постають питання щодо забезпечення національної безпеки, протидії внутрішнім і зовнішнім терористичним загрозам. Одним із ключових елементів такого забезпечення є удосконалення організаційно-правових засад взаємодії та інформаційного обміну між суб'єктами боротьби з тероризмом. Визначення і закріплення у законодавстві основ правового регулювання інформаційного забезпечення діяльності суб'єктів боротьби з тероризмом сприятиме не лише ефективному виконанню покладених на кожен із суб'єктів завдань, а й реалізації комплексної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків [1].

Формування організаційно-правових основ інформаційного забезпечення діяльності суб'єктів боротьби з тероризмом, насамперед, відбувається на законодавчому рівні. Положення законів України "Про боротьбу з тероризмом", "Про Службу безпеки України", "Про Національну поліцію", "Про оперативно-розшукову діяльність", "Про контррозвідувальну діяльність", "Про інформацію" тощо визначають конститутивні засади інформаційно-правового забезпечення взаємодії суб'єктів боротьби з тероризмом. Зокрема, у ст. 8 Закону України "Про Службу безпеки України" вказано, що СБ України взаємодіє з правоохоронними та митними органами

України у порядку і на засадах, визначених законами, указами Президента України та прийнятими на їх основі актами Служби безпеки України і взаємодіє з державними органами, підприємствами, установами, організаціями та посадовими особами, які сприяють виконанню покладених на неї завдань [2]. Згідно із ст. 5 Закону України "Про Національну поліцію", поліція у процесі своєї діяльності взаємодіє з органами правопорядку та іншими органами державної влади, а також органами місцевого самоврядування відповідно до закону та інших нормативно-правових актів [3].

Важливим для формування системи організаційно-правових основ інформаційного забезпечення суб'єктів боротьби з тероризмом є положення Закону України "Про оперативно-розшукову діяльність" про те, що підрозділи, які здійснюють оперативно-розшукову діяльність, мають право знімати інформацію з каналів зв'язку, застосовувати інші технічні засоби отримання інформації; отримувати від юридичних та фізичних осіб безкоштовно або за винагороду інформацію про злочини, які готуються або вчинені, та загрозу безпеці суспільства і держави; створювати і застосовувати автоматизовані інформаційні системи тощо [4].

Інформаційне забезпечення діяльності суб'єктів боротьби з тероризмом - це насамперед цілеспрямована діяльність, яка спирається на правові, організаційні, технічні і методичні передумови щодо збору, обробки, зберігання і створення умов для використання інформації, необхідної для ефективного функціонування даної системи.

Під час проведення антитерористичних заходів діяльність суб'єктів боротьби з тероризмом становить собою складний конгломерат інформаційних зіткнень та стресових ситуацій. Для забезпечення взаємодії зазначених суб'єктів, інформація повинна відповідати таким вимогам: точності, періодичності, своєчасності, повноти, корисності, доступності.

Варто зазначити, що обмін інформацією можна розглядати як внутрішню складову управлінського процесу, і як зовнішньо й внутрішньо спрямовані зв'язки організацій та конкретних осіб, що вимагає своїх правил, методів, засобів, технологій. Виходячи з цього можемо стверджувати, що до обміну інформацією між суб'єктами боротьби з тероризмом ставляться три блоки завдань:

– забезпечення інформаційного обслуговування суб'єктів боротьби з тероризмом та інших суб'єктів, які у разі необхідності залучаються до участі у здійсненні заходів, пов'язаних з попередженням, виявленням і припиненням терористичної діяльності;

– налагодження внутрівідомчих комунікаційних каналів в процесі контактів, обміну документацією, функціонування електронних засобів зв'язку тощо;

– забезпечення взаємодії всіх суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом у межах своєї компетенції та тих, які у разі

необхідності залучаються до участі у здійсненні заходів, пов'язаних з попередженням, виявленням і припиненням терористичної діяльності.

Таким чином, взаємодію суб'єктів боротьби з тероризмом можна визначити як процес обміну інформацією, що об'єднує в єдину систему представників різних відомств; зміцнює необхідний зворотний зв'язок між ними. Вона є складним багатогранним процесом, що передбачає: забезпечення інформаційного обслуговування діяльності системи боротьби з тероризмом; налагодження тісних як внутрівідомчих так і міжвідомчих зв'язків; використання інноваційних комунікативних форм і технологій налагодження взаємодії, розвиток зв'язків з урахуванням загальної антитерористичної політики.

В процесі взаємодії здійснюється сукупність дій щодо формування й реалізації управлінських завдань і відомчих функцій, задоволення інформаційно-комунікативних потреб представників відповідних відомств на основі соціально-комунікативних технологій. Лише впорядкована, добре налагоджена взаємодія дозволяє виконувати весь спектр завдань щодо протидії тероризму.

Література

1. Постанова КМУ від 18 лютого 2016 р. № 92 Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків

2. Про Службу безпеки України: Закон України від 25.03.1992 №2229-XII [Електронний ресурс].- Режим доступу: http://zakon2.rada.gov.ua/laws/show/2229-12.

3. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. – Верховна Рада України. – Офіційний веб-сайт. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/580-19.

4. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII. – Верховна Рада України. – Офіційний веб-сайт. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2135-12.

УДК 305 : 351.746.1

Чеховська М.М.
доктор економічних наук, професор
Національна академія Служби безпеки України

ГЕНДЕРНА ПЕРСПЕКТИВА У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Важливою передумовою для забезпечення національної безпеки держави, у тому числі її інформаційної складової, є створення можливостей для усіх громадян країни, у тому числі й жінок, обіймати посади у сфері забезпечення інформаційної безпеки.

Наголосимо, що за кордоном популяризація роботи в ІТ-індустрії здійснюється за багатьма напрямами – від проведення професійних конкурсів до оприлюднення виступів керівників спецслужб щодо активізації залучення до роботи у сфері кібербезпеки.

Так, голова MI-6 сер Алекс Янгер зазначив, що премія «Women in IT Awards» визначає внесок жінок у розвиток ІТ-індустрії та їхньої ролі в удосконаленні діяльності секретної розвідувальної служби [1]. Разом з тим він наголосив, що гендерний дисбаланс став каменем спотикання для тих, хто зацікавлений у справедливому та ефективному суспільстві. Жінки, незважаючи на корпоративні зобов'язання щодо поліпшення гендерної різноманітності, продовжують втрачати свої позиції в галузі інформатики та інформаційних технологій.

Виступаючи на конференції CyberUK в Манчестері, директор з комунікацій Національного центру кібербезпеки Великобританії (The National Cyber Security Centre, NCSC) Нікола Хадсон сказав, що для створення більш безпечної цифрової Британії необхідно створити інноваційну, різноманітну і гнучку кібер-індустрію, до роботи в якій залучатиметься більш різноманітна робоча сила. Зазначимо, що Хадсон привітав кроки NCSC як організації, яка сповнена рішучості поглянути на різноманітність в найширшому сенсі та не лише створювати робочі місця для жінок, а й враховувати соціально-економічні фактори, регіональні та культурні відмінності, гендерні аспекти самоідентифікації сучасної британської спільноти [2].

Загалом дослідники зазначають, що жінки становлять лише 11 % робочої сили у сфері інформаційної безпеки, і цей відсоток залишається стабільним з 2013 року. Крім того, близько 85 % жінок стикалися з певним рівнем дискримінації на професійних конференціях з інформаційної безпеки, а більше половини зазнали домагань на цих заходах [3].

Цікаво, що на сьогоднішній день рівень освіти жінок у сфері інформатики та інженерії дає їм можливість скоротити розрив з чоловіками у забезпеченні інформаційної безпеки. Крім того, жінки вступають в галузь з більш високим рівнем освіти, ніж чоловіки, адже 51% жінок мають ступінь магістра або вище із спеціалізацій, пов'язаних із кібербезпекою, в порівнянні з 45% їхніх колег-чоловіків [4].

Шляхами встановлення пропорційного залучення жінок та чоловіків до роботи у сфері інформаційної безпеки іноземними дослідниками, зокрема Джейн Франкленд, визначаються наступні [3]:

- здійснення найму на роботу більшої кількості жінок, адже згідно із дослідженнями, різноманітні робочі групи працюють краще і дають кращі результати, а безпосередньо жінки привносять іншу, альтернативну точку зору у бачення забезпечення інформаційної безпеки;

- залучення жінок до наставництва, адже наставництво – це привабливий спосіб ознайомитися з інформаційною безпекою і зробити її цікавою для групи людей, які не є домінуючими за якоюсь ознакою, зокрема статтю, у певному середовищі;

- підтримувати співробітництво жінок із структурами, що реалізують принципи гендерної рівності, зокрема Women's Society of Cyberjutsu (WSC), Women in Cyber Project, та Women in Cyber Security (WiCyS);

- заохочувати дівчат та жінок вивчати можливості інформаційної безпеки.

Загалом, на нашу думку, необхідним є запровадження так званої моделі «дійсної рівності», тобто рівності можливостей, рівності в доступі до можливостей та рівноцінності результатів. Така модель має бути впроваджена в усіх сферах не лише національної економіки, а й у секторі безпеки та оборони держави. Саме залучення професіоналів, як жінок, так і чоловіків, надасть більший спектр можливостей для реалізації поставлених завдань.

Використовуючи збільшення інтересу жінок до сучасних технологій та залучаючи молодих дівчат через освітні програми до подальшої роботи у секторі безпеки, досить реальним було б скорочення дефіциту робочої сили, зокрема, у сфері забезпечення інформаційної безпеки.

Вкрай важливо, щоб індустрія інформаційної безпеки передбачала довгострокові тенденції у процесі прийому на роботу, з тим, щоб отримати вигоду з переваг, які можуть у подальшому надати жінки, адже занадто часто кібербезпека сприймається як суто «чоловічий світ», і молоді жінки потребують додаткової інформації щодо наявності освітніх програм і можливостей розвитку професійної кар'єри, в якій поки домінують чоловіки.

Література

1. Martin Alexander J. N real life, Q is a woman! Head of MI6 calls for more female techies at SIS. URL : https://www.theregister.co.uk/2017/01/26/in_real_life_q_is_a_woman_head_of_mi6_calls_for_more_lady_techies_at_sis/. (дата звернення 02.03.2019).

2. Raywood D. #CyberUK: NCSC Says Diversity Will Aid a Safer Britain. URL: https://www.infosecurity-magazine.com/news/cyberuk-ncsc-diversity-aids-safer/. (дата звернення 02.03.2019).

3. Francen E. Gender Inequality in Information Security. URL: https://www.infosecurity-magazine.com/opinions/gender-inequality-security/. (дата звернення 02.03.2019).

4. Cobb Johnson M. We Must Attract Women into Cybersecurity to Close the Skills Gap #IWD2018. URL: https://www.infosecurity-magazine.com/blogs/women-close-skills-gap/. (дата звернення 02.03.2019).

УДК 351.86(477)
Шиповський В.В.
Національний університет оборони України
ім. Івана Черняховського

АНАЛІЗ ІНФОРМАЦІЙНО-ПРОПАГАНДИСТСЬКИХ ДІЙ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ

Сфера забезпечення національної безпеки та оборони будь-якої держави, в першу чергу, залежить від своєчасного виявлення актуальних загроз та вироблення ефективних та реальних стратегій протидії таким загрозам. Аналіз ходу ведення сучасних війн свідчить, що інформаційне протистояння між сторонами конфлікту є однією з найважливіших складових стратегії застосування "м'якої сили", при цьому така складова одночасно використовується як елемент підготовки до застосування, а також як один з елементів всебічного забезпечення застосування "жорсткої сили".

Одним з методів досягнення визначених цілей, який намагається реалізувати Російська Федерація у ході інформаційного протистояння з Україною, – є застосування заздалегідь спланованого, комплексного, гнучкого, масованого впливу на такий елемент суспільної свідомості як історична спадщина, активно застосовуючи засоби масової інформації та соціальні мережі.

Метою такого впливу є викривлення причинно-наслідкових зв'язків у історичній свідомості народу, що сприяє створенню або ескалації внутрішніх конфліктів. Іншими словами, противник, до якого застосовується такий метод впливу, позбавляється історичного досвіду. Масово застосовується тактика залякування, формування в історичній свідомості противника альтернатив можливого розвитку подій із найбільш трагічними, кривавими епізодами в його історії.

До власного населення, як і до світової спільноти, застосовується інша стратегія: спотворення реального сприйняття дій та намірів противника, формування його суті із вкрай негативними якостями, які необхідно знищити або, принаймні, блокувати, без заощаджень ресурсів та з використанням усіх можливих засобів.

Щодо маніпуляцій історичною свідомістю, широко використовується той факт, що вдосконалення інформаційних засобів, охоплення інформаційними мережами практично усіх верств населення, миттєве розповсюдження інформації в таких мережах, – усе це трансформувало історичну науку в інформаційний продукт масового споживання, що практично не піддається модерації з боку істориків.

Визначаючи особливості прийомів інформаційно-пропагандистської війни Росії проти України, можна зазначити наступні риси інформаційного впливу:

по-перше, виділено три основні цільові групи: населення України, населення Росії, державні діячі Заходу. Для кожної з яких визначені такі ці-

лі: головна мета інформаційної війни в Україні – ліквідація державності України; в Росії – отримання підтримки населення для виправдання дій керівництва Росії; для країн Заходу – дискредитація дій керівництва України та її Збройних Сил;

по-друге, інформаційна війна розпочалась задовго до військової агресії Росії проти України та продовжує супроводжувати її на всіх етапах, завчасно адаптуючись під поточні задачі та зміни ситуації;

по-третє, інформаційно-пропагандистські та дезінформаційні проекти, операції і заходи скоординовані та узгоджені між усіма інформаційними каналами з боку Росії.

Не врахування досвіду інформаційно-пропагандистських дій Російської Федерації проти України, призведе до затягування часу у вирішенні конфлікту, що негативно відобразиться на європейських та євроатлантичних перспективах України. Протистояти російській інформаційно-пропагандистській діяльності можливо та необхідно лише у тісній взаємодії з інформаційними ресурсами демократичних країн Заходу, спрямовуючи та координуючи спільну роботу не тільки щодо роз'яснення поточних російських інформаційних акцій, а й на їх упередження та активну протидію.

УДК 34 (477); 342.7

Щербина Л.І.
кандидат юридичних наук,
старший науковий співробітник,
Національна академія Служби безпеки України

ЩОДО ПРОБЛЕМНИХ ПИТАНЬ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ

Інформаційний простір, основними компонентами якого є інформаційні ресурси, засоби інформаційної взаємодії та інформаційна інфраструктура, представляє собою сферу сучасного суспільного життя, в якій інформаційні комунікації відіграють провідну роль. Об'єктивним процесом є поступове, але неухильне входження вітчизняного інформаційного простору до європейської та світової інформаційної сфери, в контексті чого постає закономірне питання щодо його захисту, як однієї із складових захисту національної безпеки України. Але реалізація зазначеного питання на практиці відразу стикається з необхідністю дотримання гарантованих міжнародними нормативно-правовими актами і Конституцією України прав та основоположних свобод людини, насамперед у сфері доступу до інформації.

Право на доступ до інформації є конституційним правом людини, яке передбачене і гарантоване ст. 34 Конституції України, а саме: право кож-

ного на свободу думки і слова, на вільне вираження своїх поглядів і переконань; право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб на свій вибір. Здійснення цих прав може бути обмежене лише у визначених законом випадках, проте, положення ч. 2 ст. 15 Конституції України містить імперативну норму, що цензура в державі заборонена.

Вирішення означеного проблемного питання, на нашу думку, потребує з'ясування сутності вказаної категорії. Так, поняття цензури (лат. *censura* – «суворе судження», «принципова критика») не має універсальної дефініції і, здебільшого, сприймається виключно як негативне соціокультурне явище. Разом з цим, усі розвинуті демократичні держави мають певний цензурний режим.

Зазвичай під цензурою розуміють систему контролю владних інституцій за змістом і розповсюдженням інформації у вигляді друкованої продукції, музичних і сценічних творів, творів образотворчого мистецтва, кіно-, фотоматеріалів, передач радіо і телебачення, веб-ресурсів, а в окремих випадках – приватного листування, з метою обмеження або недопущення поширення ідей і відомостей, визнаних шкідливими, небажаними для держави або суспільства в цілому.

Як соціокультурний феномен цензура має складну типологічну структуру. За змістом інформації, що підлягає контролю, фахівці поділяють її на військову, державну, економічну, комерційну, політичну, ідеологічну, моральну та духовну. Вона також поділяється на світську та релігійну, а за типом носіїв – на цензуру періодичних друкованих видань, книг, театру, кіно, публічних виступів тощо.

Цензура буває відкритою, коли встановлюється пряма заборона на публікацію або інше оприлюднення небажаної для держави, суспільства або інших інституцій інформації, та прихованою – у вигляді психологічного впливу на громадян, спрямованого на те, щоб вони утрималися від висловлювання або підтримки певних ідеї, поглядів тощо.

За способами здійснення відкрита цензура поділяється на попередній та наступний контроль. Так, при попередньому контролі передбачено отримання дозволу на оприлюднення тієї чи іншої інформації, а при наступному – оцінюється вже оприлюднена інформація, за результатами чого можуть вживатися заходи обмеження або заборони щодо обігу інформації або притягнення до відповідальності суб'єктів її поширення.

Цензура є необхідним інститутом держави, покликаним контролювати поширення інформації – найважливішого інструменту управління соціумом. Діапазон дозволеної до поширення та циркуляції в соціумі інформації залежить як від сутності самого політичного режиму, рівня демократичності влади, так і від змісту самої інформації. Частина інформації складає державну, військову, комерційну таємницю, що у свою чергу, є

об'єктивною основою для цензури. Доки є держава, зацікавлена у збереженні цих таємниць, тобто в обмеженні доступу інших осіб до певного типу інформації, до того часу в тому чи іншому вигляді буде існувати й цензура.

Історична роль і функції цензури неоднозначні. Як регулятор інформаційних потоків цензура служить одним із найважливіших механізмів захисту політичних і моральних підвалин суспільства, оскільки здатна перешкодити поширенню екстремістської, шовіністичної, расистської, націоналістичної, антисемітської, порнографічної та іншої подібної інформації, спроможної спровокувати в суспільстві відповідні негативні явища та процеси.

Водночас, за певних умов цензура може стати серйозною перешкодою на шляху до проведення прогресивних реформ та демократичного розвитку суспільства. Наприклад, інтерпретуючи дійсну й уявну новизну відповідно до догматичних установок, вона спроможна гальмувати суспільний розвиток та консервувати застарілі елементи суспільно-політичного й культурного життя держави.

З огляду на викладене, основною ознакою, за якою певне діяння може бути кваліфіковане як прояв цензури у сфері захисту інформаційного простору України, є не передбачене законом, безпідставне та необґрунтоване обмеження права особи на інформацію, яке виходить за межі визначеної для цього в ч. 2 ст. 34 Конституцій України мети – лише в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, захисту репутації або прав інших людей, запобігання розголошенню інформації, одержаної конфіденційно або для підтримання авторитету і неупередженості правосуддя.

УДК 004.056: 004.057.2

Якименко Ю.М.
кандидат військових наук,
Державний університет телекомунікацій

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ СИСТЕМНОГО МЕТОДУ СТОСОВНО ДО ПОБУДОВИ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ

Розуміння того, що організацією можна і необхідно управляти систематизовано, щоб більш ефективно досягати намічених її цілей, розвивалося протягом тривалого періоду, починаючи з середини XIX, і багато вчених в даний час продовжують пошуки, використовуючи наявні методологічні підходи в науці і техніці.

Невідповідність технологічних можливостей і методів управління стає перешкодою на шляху розвитку суспільства і всіх її інститутів і ускладнення або відсутність економічних відносин і виробничих зв'язків, невідповідність вироблених виробів (в тому числі і зразків озброєння і техніки) сучасним вимогам і способів їх використання (бойового застосування) в умовах постійно мінливої обстановки в світі та країні - все це висуває нові системні вимоги до створення або вдосконалення методології наукового дослідження.

Питання управління забезпеченням безпеки інформації стоїть у ряді найважливіших питань для будь-якої організації, а держави - найважливішим завданням. Система інформаційної безпеки (ІБ) забезпечує конфіденційність, цілісність даних, відповідність системи захисту з чинним законодавством.

Розглянемо особливості реалізації системного методу стосовно до побудови системи управління інформаційною безпекою (СУІБ) організації (підприємства, компанії).

Загальним поняттям, яке позначає всі можливі прояви систем, в тому числі і в сфері ІБ, є "системність". Центральною складовою системності є системний метод, який реалізується через свої специфічні функції - пізнавальну і методологічну. Системний метод виступає як деяка інтегральна сукупність відносно простих методів і прийомів пізнання, а також перетворення дійсності [1].

Всі організації є системами. Характер функціонування будь-якої системи пояснюють її структурою та елементами. Побудова системи здійснюється в наступній послідовності:

- формулюється мета, яка повинна забезпечуватися системою;
- визначаються функції, напрямки на досягнення цієї мети;
- створюється структура (у вигляді підсистем і взаємозв'язків між ними), що забезпечує виконання всіх функцій системи.

В Україні в більшості організацій основний упор щодо забезпечення безпеки інформації, як правило, робиться не на побудову ефективної системи ІБ, а на комплекс технічних засобів захисту інформації і розглядається як разове завдання. Однак такий підхід призводить до того, що поточний рівень безпеки організації буде недостатнім для протидії зовнішнім і внутрішнім видам загроз, які постійно змінюються. Тому ІБ повинна сприйматися як безперервний процес, інтегрований в загальну систему управління організацією, а побудова ефективної системи ІБ і її подальше вдосконалення перебувати в постійній увазі керівництва.

В Україні застосовуються міжнародні стандарти з ІБ, в яких викладені основні вимоги щодо побудови і правилам використання систем забезпечення безпеки інформації.

Вимоги національних українських документів по ІБ орієнтовані в першу чергу на державні структури і практично не враховують реалій сучасного бізнесу. У приватному бізнесі враховуються завжди його можливості по виділенню фінансових коштів для забезпечення необхідного рівня безпеки, які впливають на досягнення основної мети бізнесу - отримання прибутку.

Найбільш ефективним вирішенням завдань ІБ в організації є СУІБ [2]. В основу побудови СУІБ покладено класичну модель безперервного поліпшення процесів Шухарта-Демінга - PDCA. Стандарт ISO/IEC 27001 висуває загальні вимоги до побудови системи менеджменту (управління) інформаційною безпекою на її основі і розглядає цю модель як основу функціонування всіх процесів систем управління в сфері ІБ, тим самим досягається комлексність і повне охоплення заходів по організації забезпечення безпеки. СУІБ може бути представлена у вигляді моделі процесів ІБ. До таких систем управління в сфері ІБ відносяться системи: управління ризиками ІБ, управління інцидентами ІБ, захисту інформації, моніторингу подій і аудиту ІБ. Процес управління в цих системах включає основні етапи:

- виявлення, збір даних про події та їх аналіз, планування і підготовка заходів;
- реалізація запланованих заходів і оцінка подій (наслідків);
- прийняття рішень і усунення негативних причин (розслідування);
- витяг уроків, покращення, вдосконалення процесів та рекомендації щодо коригування планів, складання звітів про події.

За рекомендаціями експертів Інституту програмування Університету Карнегі-Меллон [3] при створенні СУІБ необхідно керуватися тим, що ефективне управління ІБ бізнесу характеризуються ознаками:

1. Охоплення всього підприємства.
2. Відповідальність керівників.
3. ІБ розглядається в якості вимоги бізнесу.
4. ІБ забезпечується з урахуванням ризиків.
5. Визначено ролі і розділені зони відповідальності.
6. Адекватна політика інформаційної безпеки.
7. Достатність ресурсів, які виділяються.
8. Персонал навчений і поінформований.
9. Безпечний життєвий цикл програмного забезпечення.
10. Планована, керована і вимірювальна ІБ.
11. Регулярний аудит ІБ.

Реалізація системного методу побудови системи в сфері ІБ може бути представлена у вигляді архітектури на прикладі системи управління інцидентами інформаційної безпеки (див. рис.).

Як апаратно програмний комплекс захисту інформації пропонується використовувати IBM QRadar SIEM [4], який є однією з найбільш ефекти-

вних аналітичних систем безпеки для захисту інформації від різних видів загроз ІБ. Рішення QRadar SIEM підтримує роботу з більш ніж 200 продуктів від провідних виробників і проводить збір, аналіз і кореляцію даних через широкий спектр систем, включаючі мережеві рішення, засоби безпеки, сервери, хости, операційні системи і додатки.

Платформа QRadar Security Intelligence Platform має кілька модулів, основні з них:

- QRadar SIEM, Log Manager (управління журналами),
- Risk Manager (управління ризиками), Vulnerability Manager (управління уразливостями).

Реалізація системного методу побудови СУІБ і використання в ній IBM QRadar SIEM дозволить підвищити результативність захисту інформації.

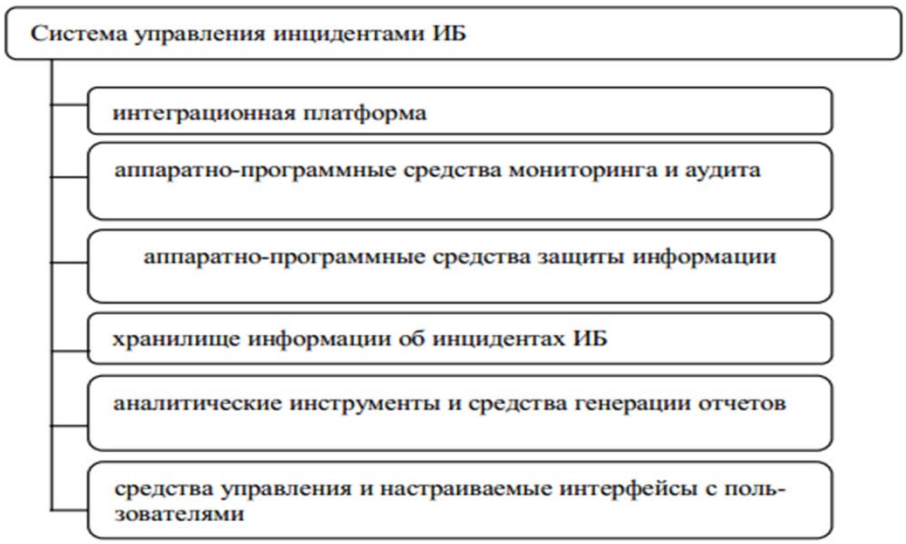


Рис. 1. Архитектура системы управления инцидентами ИБ

Література

1. Исследование систем управления.Учебно-методический комплекс по дисциплине.- Липецк: 2015-178с. - [Электронный ресурс]. Режим доступа: https://rucont.ru/file.ashx?guid=5246af5b-a443-4b99-a30f-34575f6f3f2e.

2. Волошин Б.В. Об особенностях построения системы управления информационной безопасностью автоматизированной системы / Б.В. Волошин Актуальные проблемы авиации и космонавтики, Том 1.- Красноярск : 2015- с.485-487. - [Электронный ресурс]. Режим доступа:

https://cyberleninka.ru/article/n/ob-osobennostyah-postroeniya-sistemy-upravleniya-informatsionnoy-bezopasnostyu-avtomatizirovannoy-sistemy.

3. Система управления информационной безопасностью бизнеса от компании Arinteg . - [Электронный ресурс]. Режим доступа: https://www.arinteg.ru/about/news/detail.php?ID=134443.

4. IBM Security QRadar. Version 7.2.8. User Guide.- [Електронний ресурс]. Режим доступу: https://www-01.ibm.com/support/docview.wss?uid=swg27048741.

УДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА УКРАЇНИ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ

УДК 341.824:338.47 (043.2)
Богомолов О.О.
Воєнно-дипломатична академія
ім. Євгенія Березняка

РОЗРОБКА ТА ВПРОВАДЖЕННЯ СУЧАСНОЇ СИСТЕМИ БЕЗПЕКИ СЕКРЕТНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА АВТОМАТИЗАЦІЯ РЕЖИМНО-СЕКРЕТНОЇ ДІЯЛЬНОСТІ

В умовах глобалізації інформаційного обміну і широкого впровадження інформаційних технологій в усіх сферах життєдіяльності суспільства України існує проблема захисту інформації, що обробляється в інформаційних, інформаційно-телекомунікаційних та автоматизованих системах (далі – ІТС), від викликів і загроз у кібернетичному та віртуальному просторі, а також від зловмисних дій порушника.

З метою їх реалізації Верховною Радою України були прийняті закони України [1-5], які окреслюють основні організаційно-правові засади електронного документообігу та використання електронних документів, зокрема закріплено визначення та юридичний статус електронного документу. Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму. Електронний цифровий підпис дає змогу підтвердити цілісність електронного документу.

Розробка та впровадження сучасної системи безпеки секретних інформаційних ресурсів (далі – СІР) та автоматизація режимно-секретної діяльності (далі – РСД) дозволить налагодити моніторинг стану захищеності як матеріальних так і електронних секретних ресурсів будь-якої установи або організації, яка впроваджує діяльність, пов’язану з державною таємницею або іншою інформацією з обмеженим доступом.

В доповіді розкриті наступні питання:

1) впровадження системи безпеки СІР на кожному окремому суб’єкті провадження РСД за єдиними стандартами;

2) реалізація в системі безпеки СІР сучасних технічних рішень автоматизації управлінської діяльності;

3) провадження єдиної політики надання доступу до державних секретів (секретної інформації), їх матеріальних носіїв та/або електронних відображень (ресурсів);

4) надання дозволу органам безпеки державних секретів (далі – ОБДС) на створення систем автоматизації РСД, визначення комплекту програмного забезпечення, програмно-апаратних комплексів, гаджетів тощо;

5) впровадження незалежного контролю (аудиту) за недопущенням несанкціонованого доступу до СІР та упередження утворення можливих каналів їх витоку.

Серед основних принципів, які визначають шляхи створення системи безпеки СІР визначені наступні:

єдність підходів щодо утворення політики безпеки СІР;

обов'язковість досліджень ефективності заходів усунення недоліків систем захисту інформації;

комплектність, повнота та безперервність заходів системи аудиту безпеки СІР;

наближеність процедур оцінки ефективності заходів та засобів захисту інформації до стандартів НАТО і ЄС;

забезпеченість нормативно-правовими документами щодо діяльності спеціалістів із захисту державних секретів та адміністраторів безпеки ІТС.

Реалізація системи безпеки СІР повинна включати наступні етапи:

етап формування правової основи створення системи безпеки СІР;

етап створення ОБДС в системі захисту державних секретів;

етап впровадження електронного секретного документообігу управлінської діяльності;

етап впровадження порядку утворення та супроводження Реєстру споживачів СІР, створення захищеного банку даних нормативно-правової, довідково-інформаційної та управлінської діяльності;

етап створення Центру з сертифікації та забезпечення ключовими даними та НКІ;

етап сертифікації системи безпеки СІР.

Література

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.94 № 80/94-ВР // База даних «Законодавство України / ВР України». URL: http://zakon3.rada.gov.ua/laws/show/80/94-вр (дата звернення 04.03.2019).

2. Про державну таємницю: Закон України від 21.01.94 № 3855-XII // База даних «Законодавство України / ВР України» URL: http://zakon1.rada.gov.ua/laws/show/3855-12 (дата звернення 04.03.2019).

3. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV // База даних «Законодавство України / ВР України». URL: http://zakon1.rada.gov.ua/laws/show/851-15 (дата звернення 04.03.2019).

4. Про електронний цифровий підпис: Закон України від 22.05.2003 № 852- IV // База даних «Законодавство України / ВР України» URL: http://zakon1.rada.gov.ua/laws/show/852-15 (дата звернення 04.03.2019).

5. Про Національну програму інформатизації: Закон України від 04.02.98 № 74/98-ВР // База даних «Законодавство України / ВР України» URL: http://zakon1.rada.gov.ua/laws/show/74/98-вр (дата звернення 04.03.2019).

УДК 007.65.01
Вдовенко С.Г.
Даник Ю.Г.
доктор технічних наук, професор
Національний університет оборони України

ЗАКОНОДАВЧІ ТА НОРМАТИВНО-ПРАВОВІ АСПЕКТИ ПРОБЛЕМ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ І СЛУЖБОВОЇ ІНФОРМАЦІЇ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Досвід збройних конфліктів початку XXI століття, в тому числі операцій на території України [1] свідчить про зростання вимог до організаційно-технічних засад забезпечення безпеки інформації, яка циркулює в інформаційному просторі при вирішенні задач управління військами. Забезпечення охорони державної таємниці (ОДТ), поряд з криптографічним і технічним захистом інформації (КЗІ, ТЗІ), протидією технічним розвідкам є однією з основних складових частин скритого управління військами (СУВ) [2].

Суспільні відносини, пов’язані з ОДТ, як складової національної безпеки України (НБ) регулюються Законом [3], відповідно до вимог якого у ЗС України створена та діє система ОДТ, яка складається з підсистем: режиму секретності та секретного документального забезпечення; захисту інформації (КЗІ і ТЗІ) та підсистеми технічного забезпечення [4]. Діяльність МО України та ЗС України регламентується Законами, якими визначені особливі повноваження щодо провадження державної політики у сфері оборони, у тому числі, з урахуванням [3, ст. 8], в частині що стосується ОДТ [8, ст. 3; 9, ст. 11].

Однією із загроз НБ визнана фізична і моральна застарілість системи ОДТ та інших видів інформації з обмеженим доступом (ІзОД) [5, 6]. Концепція [7] визначає сектору безпеки і оборони завдання щодо забезпечення ОДТ, ІзОД, удосконалення керівництва системою захисту інформації. Стратегією [6] реформування системи ОДТ визнано пріоритетним завданням забезпечення кібербезпеки (КБ) і безпеки інформаційних ресурсів.

Існують серйозні протиріччя між законодавчою та нормативно-правовою базами України у сфері ОДТ, сучасними вимогами щодо захисту ІзОД з урахуванням досвіду ЄС та НАТО. Закон [3, ст. 5] на Раду національної безпеки і оборони України (РНБО), Кабінет Міністрів (КМ)

України покладає повноваження щодо спрямування, координації та контролю діяльності державних органів із забезпечення реалізації державної політики у сфері ОДТ, які фактично зараз виконуються СБУ, що є спеціально уповноваженим державним органом у сфері забезпечення ОДТ [3, ст. 5, ст. 37]. Таким, чином між [3, ст. 5, ст. 37] та [13, ст. 32; 5, ст. 4],Указом [14, п. 5] закладені системні протиріччя. Між [3, ст. 5, ст. 21] та [13, ст. 2, ст. 19] закладені протиріччя стосовно покладання завдань щодо забезпечення та здійснення ОДТ, відповідно, на керівників та на РСО, або на СБУ. Закон [3] визначає ОДТ як комплекс заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв. Значна частина таких заходів віднесена до повноважень Державної служби спеціального зв'язку та захисту інформації України (ДССЗІУ) [18]. Дефініція "забезпечення ОДТ" законодавчо, або нормативно не визначена. Закон України [3] прийнято у 1994 році. За цей час в державі відбулася низка організаційно-структурних та нормативно-програмних змін закріплених в [5, 6, 7, 10, 11, 15], що поглибили протиріччя. Як приклад, суперечливість Закону [15, ст. 2, п. 2)] щодо його не поширення на діяльність, пов'язану із захистом інформації, що становить державну таємницю, та завданнями, визначеними в [6, п.п. 3.2, 3.7, 4.2, 4.4, 4.12; 7. розділи I, II, III]. Система ОДТ не є складовою частиною кібербезпеки (КБ), але, як і КБ, є складовою частиною інформаційної безпеки (ІБ). Заходи ІБ виконуються і в мирний час і в особливий період. А Постанова КМ України [19] не включає спеціальність "ІБ" та визначає у галузі знань "Інформаційні технології" лише спеціальність "КБ". Такий стан вимагає не лише певних змін, а докорінного реформування системи ОДТ. Зміни запропоновані проектами Законів України "Про охорону секретної інформації" та "Про КЗІ та ТЗІ", не вирішують проблеми об'єктивно та комплексно. На наш погляд, на відміну від існуючої системи ОДТ, основною парадигмою має стати захист ІзОД [12], що відповідає вимогам ЄС та НАТО, які передбачають в НАТО і кожній державі-члені НАТО мати урядове бюро національної безпеки (national security organization – NSO), що відповідає за ІБ та персонал, а також за збір і реєстрацію відомостей щодо шпигунства та підривної діяльності, та яке не входить до інших державних структур.

З огляду на зазначене з метою вирішення проблем у сфері ОДТ (захисту ІзОД) в державі вважається за доцільне (пропонується):

1. Здійснити усунення невідповідностей шляхом законодавчого, нормативно-правового й дефініційного врегулювання у сфері НБ, ОДТ (захисту ІзОД) та КБ, зокрема у [2,3,6,7,8,16]. У встановленому порядку розглянути пропозиції щодо внесення змін до [3] щодо дозвільної та допускної систем.

2. Розробити Концепцію розвитку системи ІзОД (К) держави та на її підставі - Державну програму розвитку системи захисту ІзОД (ДП), яку

після розгляду в РНБО затвердити Постановою КМ відповідно до Закону [17]. До виконання завдання залучити ДССЗІУ, СБУ, ГШ ЗС України, науково-дослідні установи. Передбачити заходи щодо: визначення переліку напрямів наукових досліджень та профільних науково-дослідних установ в галузі ЗІ; розвиток систем ТЗІ та КЗІ; визначення порядку і джерел фінансування фундаментальних наукових досліджень, НДДКР тощо;

3. Опрацювати питання стосовно покладання завдань з координації робіт щодо забезпечення здійснення державної політики в сфері ОДТ (ІзОД) на спеціально уповноважений орган виконавчої влади з питань захисту ІзОД, захисту державних інформаційних ресурсів, систем електронного врядування, ТЗІ і КЗІ, який повинен бути безпосередньо підпорядкований КМ України**.**

Література

1. Закон України від 18 січня 2018 року № 2268-VIII Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях(Відомості Верховної Ради (ВВР), 2018, № 10, ст. 54)

2. Звід відомостей, що становлять державну таємницю, затверджений наказом СБУ від 12.08.2005 №440, зареєстрований в Міністерстві юстиції України 17.08.2005 за № 902/11182, зі змінами.

3. Закон України "Про державну таємницю" від 21 січня 1994 року № 3855-XII, зі змінами (Відомості Верховної Ради України (ВВР), 1994, № 16, ст. 93).

4. Вдовенко С.Г. Сучасні вимоги до охорони державної таємниці та захисту інформації з обмеженим доступом в особливий період / Імперативи розвитку цивілізації – 2015 – №2. Київ – ФОП О.С.Ліпкан, С. 93-96.

5. Закон України Про національну безпеку України від 21 червня 2018 року № 2469-VIII (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241)

6. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015.

7. Концепція розвитку сектору безпеки і оборони України, введена в дію Указом Президента України від 14.03.2016 №92/2016.

8. Закон України "Про оборону України" від 6 грудня 1991 року № 1932-XII, зі змінами (Відомості Верховної Ради України (ВВР), 1992, № 9, ст. 106).

9. Закон України "Про Збройні Сили України" від 6 грудня 1991 року № 1934-XII, зі змінами (Відомості Верховної Ради України (ВВР), 1992, № 9, ст. 108) http://zakon3.rada.gov.ua/laws/show/1934-12.

10. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України" від 23 лютого 2006 року № 3475-IV зі змінами (Відомості Верховної Ради України (ВВР), 2006, № 30, ст. 258).

11. Конституція України. http://zakon0.rada.gov.ua/laws/show/254.

12 Вдовенко С.Г. Даник Ю.Г., Концептуальні напрями комплексного вирішення проблеми захисту інформації в системі скритого управління Збройних сил / Сучасні інформаційні технології у сфері безпеки та оборони № 2(29). – 2017. – С. 98-106.

13. Закон України "Про Службу безпеки України" від 25 березня 1992 року № 2229-XII зі змінами (Відомості Верховної Ради України (ВВР), 1992, № 27, ст. 382).

14. Указ Президента України Про посилення контролю за діяльністю Збройних Сил України та інших військових формувань від 14.02.2015 року № 84/2015.

15. Закон України "Про основні засади забезпечення кібербезпеки України" від 5 жовтня 2017 року № 2163-VIII, зі змінами, (Відомості Верховної Ради (ВВР). – 2017. – № 45. – Ст. 403).

16. Стратегічний оборонний бюлетень України, введений в дію Указом Президента України від 6 червня 2016 року № 240/2016.

17. Закон України "Про Кабінет Міністрів України" від 27 лютого 2014 року № 794-VII, зі змінами (Відомості Верховної Ради (ВВР). – 2014. – № 13. – Ст. 222).

18. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України" від 23 лютого 2006 року № 3475-IV (Відомості Верховної Ради України (ВВР). – 2006. – № 30. – Ст. 258).

19. Постанова Кабінету Міністрів України Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти від 29 квітня 2015 р. № 266.

УДК 35.078.3:342.739 (091)

Гуз А.М.
доктор історичних наук, професор
Національна академія Служби безпеки України

ІСТОРИЧНІ ПЕРЕДУМОВИ ПРАВОВОГО РЕГУЛЮВАННЯ ОХОРОНИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ НАТО ТА УКРАЇНИ

Одним з пріоритетних напрямів зовнішньої політики України є розвиток партнерства з Організацією Північноатлантичного договору. Відносини НАТО з Україною почали розвиватися невдовзі після проголошення незалежності у 1991 році. Оскільки Україна активно включилася у співпрацю з НАТО, то природно постало питання щодо охорони інформації з обмеженим доступом двох сторін. З метою створення правових засад для обміну інформацією з обмеженим доступом, який здійснювався між органами державної влади, установами України та НАТО в рамках відповідних програм співробітництва, 13 березня 1995 року у м. Брюссель було укладено «Угоду про безпеку між Урядом України і Організацією Північноатлантичного Договору» (ратифіковано Законом № 160-IV від 12.09.2002)[1]. Зазначена Угода, зокрема передбачала: здійснення між Україною та НАТО консультацій і обміну інформацією з обмеженим доступом з політичних питань та питань, пов'язаних з безпекою, а також інтенсифікацію політичного та військового співробітництва; захищати інформацію та матеріали іншої сторони; не використовувати отриману в результаті обміну інформацію та матеріали в цілях, відмінних від тих, що встановленні в рамках відповідних програм, а також рішень та резолюцій,

що стосуються таких програм; не надавати таку інформацію та матеріали третім сторонам без згоди Сторони-джерела [1].

З метою практичної реалізації вказаного міжнародного договору, Службою безпеки України в односторонньому порядку були розроблені «Правила поводження та забезпечення охорони інформації НАТО з обмеженим доступом в Україні», які затверджено СБ України в 2002 році. Довгий час саме на підстави цього документа здійснювалася охорона інформації з обмеженим доступом НАТО і України.

З метою деталізації процедур із забезпечення безпеки інформації з обмеженим доступом відповідно до статті 4 Угоди про безпеку між Урядом України і Організацією Північноатлантичного Договору, а також визначення правових засад забезпечення взаємної охорони інформації з обмеженим доступом 28 вересня 2016 року підписано Адміністративні домовленості щодо охорони інформації з обмеженим доступом між Урядом України та Організацією Північноатлантичного Договору. Цей документ ратифікований Законом України від 24 травня 2017 року № 2068-VIII і набрав чинності для України 4 серпня 2017 року [2]. Зазначений документ закріплює на міжнародному рівні зобов'язання сторін і детальний порядок охорони інформації з обмеженим доступом, обмін якою здійснюється між Україною та НАТО. Зокрема, у положеннях Адміністративних домовленостей: визначаються формат, статус та сфера дії цього міжнародного документу; охарактеризовано органи безпеки, відповідальні за їх імплементацію цього документа, а саме: СБУ та Офіс безпеки НАТО, які забезпечують впровадження мінімальних стандартів охорони та поводження з інформацією з обмеженим доступом, обмін якою здійснюється між Україною та НАТО та забезпечують нагляд за їхнім дотриманням, сприяють проведенню взаємних перевірок з метою досягнення впевненості, що передана будь-якій стороні інформація належним чином захищена; проведено співставлення грифів обмеження доступу для застосування рівнозначних заходів охорони інформації, обмін якою здійснюватиметься між сторонами; визначено мінімальні стандарти безпеки, за якими сторони зобов'язуватимуться забезпечувати взаємну охорону інформації з обмеженим доступом, зокрема у сферах допускної системи, фізичної безпеки, ведення діловодства, технічного захисту інформації тощо; окреслено статус та роль Місії України при НАТО, яка діє як первинний пункт входу до України інформації НАТО з обмеженим доступом [2].

Ратифіковані Адміністративні домовленості створили підставу для перегляду та оновлення «Правила поводження та забезпечення охорони інформації НАТО з обмеженим доступом в Україні», які регулювали сферу охорони інформації з обмеженим доступом НАТО та України майже 14 років. Нові «Правил забезпечення охорони інформації НАТО з обмеженим доступом в Україні» були розроблені та введені в дію СБ України у

січні 2018 року. Цим документом враховано запроваджені Адміністративними домовленостями нововведення щодо термінології та вимог з охорони інформації з обмеженим доступом, які відповідають безпековим стандартам НАТО. В нових Правилах оптимізовано процедури щодо: порядку маркування обмежувальними позначками документів НАТО згідно з еквівалентністю грифів обмеження доступу, встановленою Адміністративними домовленостями; механізмів обміну інформацією НАТО в рамках реєстраційної системи; вимог надання доступу до інформації НАТО та опрацювання документів, що містять таку інформацію; процедур відтворення та знищення матеріальних носіїв інформації НАТО з обмеженим доступом; особливостей контролю за станом забезпечення охорони інформації, обмін якою здійснюється тощо.

Таким чином можемо з упевненістю констатувати, що за понад 20 років співробітництва України з НАТО у сфері охорони інформації з обмеженим доступом створено дієву систему, яка постійно удосконалюється реагуючі на сучасні загрози національній безпеці та у відповідності до вимог сьогодення.

Література

1. Угода про безпеку між Урядом України і Організацією Північноатлантичного Договору (Угоду ратифіковано Законом № 160-IV (160-15) від 12.09.2002) / Законодавство України//https://zakon.rada.gov.ua/lows/ документ 950_002.

2. Адміністративні домовленості щодо охорони інформації з обмеженим доступом між урядом України та Організацією північноатлантичного договору від 28.09.2016 (Адміністративні домовленості ратифіковано Законом № 2068-VIII від 24.05.2017)/Законодавство України// https://zakon.rada.gov.ua/lows/ документ950_035-16.

УДК 341

Зуб О.О.
Служба безпеки України

УДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА УКРАЇНИ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ З УРАХУВАННЯМ СТАНДАРТІВ БЕЗПЕКИ НАТО ТА ЄС

У контексті впливу зовнішніх та внутрішніх чинників на стале функціонування держави найбільш уразливою є чутлива інформація, доступ до якої обмежується в інтересах держави, та яка підлягає її охороні, тобто державна таємниця та службова інформація.

Враховуючи взятий нашою країною курс на інтеграцію в євроатлантичний простір, іноземними партнерами очікується від України вжиття відповідних заходів, спрямованих на вироблення нових підходів щодо забезпечення безпеки згаданих вище видів інформації.

З цією метою положеннями Стратегії національної безпеки України, яку затверджено Указом Президента України від 26.05.2015 № 287/2015, передбачено необхідність реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом з урахуванням практики держав-членів НАТО та ЄС.

В рамках реалізації положень Стратегії Службою безпеки України як спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці розпочато роботу з адаптації та гармонізації національного законодавства до стандартів безпеки НАТО та ЄС.

Виходячи з важливості зазначеного питання, яке безпосередньо стосується національної безпеки України, впровадження певних новацій потребує виваженого підходу та ретельного вивчення практики їх застосування в інших державах. Тому, у Службі безпеки України проведено аналіз стандартів безпеки НАТО та ЄС, а також вивчено досвід країн євроатлантичної спільноти, які пройшли шлях реформування національного законодавства у сфері охорони інформації з обмеженим доступом за схожих з Україною умов.

За результатами проведеного аналізу з'ясовано, що в державах-членах НАТО та ЄС інформація з обмеженим доступом охороняється шляхом застосування збалансованого ряду заходів безпеки, що ґрунтуються на таких базових компонентах як безпека персоналу, фізична безпека, адміністрування секретного діловодства, промислова безпека, безпека комунікаційно-інформаційних систем.

Також, стандартами безпеки НАТО та ЄС для побудови системи охорони інформації з обмеженим доступом:

1. Запроваджено чотирьохрівневу систему обмеження доступу до вказаної інформації, ступені якої розподіляються за рівнем шкоди, що може бути заподіяна інтересам міжнародних організацій та країн-членів у разі розголошення таких відомостей:

TOP SECRET	еквівалент	«Особливої важливості»
SECRET	еквівалент	«Цілком таємно»
CONFIDENTIAL	еквівалент	«Таємно»
RESTRICTED	еквівалент	«Для службового користування»

2. Передбачено, що кожна держава-член, партнери НАТО визначають Національні органи безпеки, відповідальні за впровадження стандартів безпеки інформації, здійснення інспектувань умов захисту інформації з

обмеженим доступом, проведення перевірок з визначення надійності громадян, які потребують доступу до секретної інформації, видачу дозволів на провадження діяльності, пов'язаної з інформацією з обмеженим доступом тощо. При цьому статус та підпорядкованість такого органу визначаються державами-членами вказаної міжнародної організації самостійно з урахуванням традиційних підходів та практики забезпечення охорони інформації з обмеженим доступом.

3. Приділено увагу питанням безпеки інформації під час виконання підприємствами недержавної форми власності контрактів або робіт, пов'язаних із секретними відомостями, та уведено поняття «промислова безпека» в рамках якої і здійснюються відповідні заходи щодо охорони секретної інформації.

4. Передбачено застосування фізичних захисних заходів щодо місць, будівель та приміщень, в яких знаходиться інформація, що потребує захисту від втрати або розголошення, тобто мають бути впроваджені заходи з фізичної безпеки. Такі заходи залежать від загроз, ступенів обмеження доступу, чутливості та кількості матеріальних носіїв інформації, що захищатимуться. Для забезпечення фізичної безпеки в усіх приміщеннях, будинках, офісах, кімнатах та на територіях, де зберігається та/або обробляється інформація з обмеженим доступом, передбачено встановлення зон безпеки інформації відповідного класу (клас I, клас II, адміністративна зона).

5. Визначено процедурні питання щодо надання доступу особам до секретної інформації в рамках здійснення заходів з безпеки персоналу.

Вказана процедура полягає у реалізації наступного підходу:

- визначення необхідності доведення до особи секретних відомостей у зв'язку з виконанням нею службових обов'язків;

- наявність сертифікату про проходження необхідних процедур з питань безпеки, спрямованих на встановлення лояльності, надійності та рівня довіри до особи;

- проведення навчань та інструктажів з питань безпеки відносно особи, якій надається доступ до секретної інформації;

- здійснення постійного контролю щодо осіб, яким оформлено такий сертифікат.

6. Впроваджено заходи щодо створення безпечного навколишнього середовища циркуляції інформації з обмеженим доступом в інформаційно-комунікаційних та інших автоматизованих системах.

З урахуванням стандартів безпеки НАТО та ЄС співробітниками СБУ спільно із фахівцями Апарату РНБО України та інших заінтересованих державних органів розроблено проект Закону України «Про охорону секретної інформації», яким планується запровадити в Україні нові підходи до безпеки інформації з обмеженим доступом, охорона якої здійснюється в інтересах держави.

Згідно з положеннями вказаного законопроекту основні зусилля у ході реформування системи охорони державної таємниці та службової інформації планується зосередити на вирішенні наступних питань:

- об'єднання державної таємниці та службової інформації в єдину категорію інформації з обмеженим доступом, визначення терміну, еквівалентного «classified information»;
- визначення на державному рівні Національного органу безпеки з покладенням всіх його функцій на Службу безпеки України;
- удосконалення процедур віднесення відомостей до секретної інформації, засекречування та розсекречування матеріальних носіїв секретної інформації;
- збільшення терміну проведення перевірки осіб у зв'язку з допуском їх до державної таємниці, диференціювання обсягу перевірки в залежності від ступеня секретної інформації, розширення переліку підстав, за яких допуск до державної таємниці не надається з урахуванням, у тому числі, вимог фінансового, антикорупційного законодавства та інших чинників, що роблять особу вразливою до тиску з боку іноземних спецслужб, терористичних та злочинних угрупувань тощо;
- впровадження нових підходів щодо фізичної безпеки інформації з обмеженим доступом шляхом поділу зон, де циркулює така інформація, залежно від умов зберігання матеріальних носіїв секретної інформації;
- оптимізація функціонування дозвільної системи;
- чітке визначення повноважень Служби безпеки України, як Національного органу безпеки, у ході проведення заходів офіційного контролю за станом охорони секретної інформації.

Вбачається, що реалізація зазначених напрямів удосконалення системи охорони державної таємниці та службової інформації дозволить забезпечити адекватне і гнучке реагування на можливі загрози безпеці такої інформації, та дозволить гармонізувати та адаптувати систему охорони державної таємниці в України до вимог стандартів безпеки НАТО та ЄС.

УДК 341.174

Касперський І.П.
кандидат юридичних наук,
старший науковий співробітник, доцент,
Національна академія Служби безпеки України

ЄВРОПЕЙСЬКІ СТАНДАРТИ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ

Прийняття у 2016 році Європейським парламентом та Радою Євросоюзу Директиви 2016/943 щодо захисту конфіденційних ноу-хау і ділової інформації (комерційної таємниці) від незаконного набуття, використання та розкриття [1] (далі – Директива) поставило перед законодавцем низку

нових завдань, виконання яких дозволить наблизити правове регулювання захисту комерційної таємниці в Україні до європейських стандартів. При цьому мова йде не тільки про виклики глобалізації, а і про прямі вимоги чинного законодавства. Відповідно до Загальнодержавної програми адаптації законодавства України до законодавства Європейського Союзу [2], однією із пріоритетних сфер, в яких здійснюється названа адаптація є сфера інтелектуальної власності. Якість правового забезпечення цього напряму набуває особливої гостроти у зв'язку із неодноразовими звинуваченнями України у системному порушенні авторських прав, що призводило до економічних санкцій з боку зокрема США [3].

Із прийняттям Директиви світова спільнота отримала дієвий інструмент гармонізації свого законодавства з метою забезпечення рівних можливостей захисту прав інтелектуальної власності своїм громадянам та зарубіжним інвесторам, що дозволить повною мірою забезпечити вільний розвиток економіки.

У преамбулі Директиви вказано, що метою її прийняття стали розбіжності у законодавстві держав-членів ЄС щодо захисту прав власників комерційної таємниці, які не дозволяють повною мірою охопити усі нюанси компенсаційних та організаційних механізмів забезпечення цих прав. Цікавим видається той аспект, що Директива містить не тільки норми щодо захисту прав інтелектуальної власності, а і запроваджує вимоги щодо неможливості використання вимог захисту комерційної таємниці для створення перешкод в діяльності органів державної влади, обмеження трудових прав громадян чи недобросовісної конкурентної боротьби. Директивою дозволено встановлювати максимальні значення компенсацій за витік комерційної таємниці для працівників, що допустили витік неумисно. Задля світового прогресу запроваджено норму, згідно із якою «зворотний інжиніринг продукту, отриманого законним шляхом, повинен розцінюватися як правомірний спосіб отримання інформації, за винятком випадків, коли договором передбачено інше» [1].

Варто наголосити, що Директива має обов'язковий характер не тільки для держав-членів ЄС, а і для усього Європейського економічного простору, тобто для усіх членів Європейської економічної асоціації, крім Швейцарії. Окремі вимоги Директиви є досить цікавими з огляду на відсутність їх аналогів у законодавстві України та доцільність їх запровадження в нашій державі.

В першу чергу це стосується детальної регламентації умов визнання набуття комерційної таємниці незаконним. До таких умов Директивою віднесено: відсутність згоди власника, яка поєднана із протиправним способом отримання даних: шляхом несанкціонованого доступу, незаконного привласнення або копіювання будь-яких документів, об'єктів, матеріалів, речовин або електронних файлів, що містять в собі комерційну таємницю,

або з яких може бути отримана комерційна таємниця. До цього переліку Директива додає обтічну норму щодо можливості визнання незаконним здобуття комерційної таємниці і шляхом «вчинення інших дій, які за наявних обставин вважаються невідповідними доброчесній комерційній практиці».

Також Директивою детально регламентуються ознаки незаконності використання комерційної таємниці, а саме незаконне здобуття цієї інформації, у тому числі отримання її від осіб, які завідомо для набувача незаконно її отримали. Незаконним також вважається використання комерційної таємниці, отриманої внаслідок порушення договірних зобов'язань.

Досить суттєвою є визначення Директивою тих обставин, які повинен брати до уваги суд, вирішуючи питання щодо відкриття провадження за позовом про порушення права на комерційну таємницю та оцінці адекватності висунутих позивачем вимог, до яких відносять:

– цінність і інші особливі характеристики комерційної таємниці;
– заходи, що вживались для захисту комерційної таємниці;
– поведінка відповідача при набутті, використанні або розкритті комерційної таємниці;
– наслідки незаконного використання або розкриття комерційної таємниці;
– законні інтереси сторін і наслідки для сторін, які могли настати в результаті застосування або відмови від застосування заходів захисту комерційної таємниці;
– законні інтереси третіх осіб;
– інтереси громадськості;
– захист основних прав.

Закріплення перерахованих норм у законодавстві України дозволить посилити захист комерційної таємниці правовими механізмами, які належно збалансовані суттєвими публічними інтересами.

Література

1. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. URL: https://wipolex.wipo.int/en/text/423032 (Date of access: 05.03.2019)

2. Загальнодержавна програма адаптації законодавства України до законодавства Європейського Союзу, затв. Законом України від 18.03.2004 р. N 1629-IV // Офіційний вісник України від 30.04.2004 — 2004 р., № 15, стор. 30, стаття 1028, код акта 28492/2004.

3. США: Україна - найбільший порушник авторського права URL: https://www.bbc.com/ukrainian/business/2013/05/130501_ukraine_us_trade_it (дата звернення 05.03.2019).

УДК 35.078.3:025.4.03+65.012.8
Князєв С.О.
кандидат юридичних наук,
старший науковий співробітник,
Національна академія Служби безпеки України

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ПЕРЕДАЧІ ДЕРЖАВНОЇ ТАЄМНИЦІ УКРАЇНИ ІНОЗЕМНІЙ ДЕРЖАВІ

Становлення та розвиток кожної держави супроводжується необхідністю постійної реалізації та розширенням її зовнішніх зв`язків, що потребує й відповідного правового врегулювання питань, які стосуються передачі різних видів інформації, у тому числі державної таємниці.

Передача такої інформації може бути пов’язана із участю у міжнародних програмах за різними сферами діяльності, проведенням спільних заходів, навчань, випуском та модернізацією озброєння й військової техніки, можливістю її подальшої реалізації тощо.

Міждержавна передача подібної інформації мусить відбуватися з метою належного забезпечення національних інтересів, здійснення цілей, завдань і принципів зовнішньої політики України, закріплених у Конституції України та законодавстві України.

Пріоритетність і складність вирішення даного питання полягає у тому, що мова йде про передачу найбільш важливої для держави інформації з обмеженим доступом - державної таємниці. При цьому складність пов’язана із необхідністю забезпечення цілого комплексу відповідних заходів.

Можливо стверджувати, що однією з основних функцій системи реалізації співробітництва України з іншими державами, у контексті використання державної таємниці, є створення необхідних правових засад регулювання режимних заходів, а також розроблення та удосконалення достатньої нормативно-правової бази, яка б регулювала відносини між державами та їх взаємодію щодо охорони державної таємниці.

На теперішній час, правову основу для можливої передачі державної таємниці України іншій державі становлять: Конституція України; Закон України «Про державну таємницю» (1994); Закон України «Про міжнародні договори» (2004); Указ Президента України «Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації» (2004); Указ Президента України «Про затвердження Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства» (2006) тощо.

Аналіз зазначених нормативно-правових актів, стосовно врегулювання процедури передачі державної таємниці іноземній державі, дозволяє виокремити та поєднати у певну послідовність наступні важливі складові:

- укладання міждержавних угод спрямованих на взаємний захист державної таємниці та їх ратифікація Верховною Радою України (або підготовка відповідного письмового мотивованого розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України);

- надання дозволу установі на передачу державної таємниці іноземній стороні;

- визначення порядку передачі державної таємниці;

- оформлення доступу до державної таємниці іноземцям;

- визначення строків, протягом яких сторони зобов'язуються забезпечувати взаємну охорону державної таємниці;

- дотримання зобов'язання щодо засекречування, зміни ступеня секретності, розсекречування секретної інформації (матеріальних носіїв такої інформації) і т.п.

Таким чином, питання пов'язані з особливостями застосування зазначених заходів регламентуються нормативно-правовими актами, які приймались у нашій державі в різний час. Разом з тим, зважаючи на динамічні процеси, які постійно відбуваються в інформаційній сфері, цілком логічним постає питання щодо узгодженості між собою даних нормативно-правових актів, врахування ними сучасної специфіки використання державної таємниці та загроз її існуванню.

У цьому контексті можливо виділити наступні пріоритетні напрями перегляду або впорядкування правового регулювання передачі державної таємниці України іноземній державі:

- використання єдиного понятійно-категорійного апарату під час укладання міждержавних договорів про взаємний захист державної таємниці, що стосується вітчизняної інформації, відповідно до законодавства України;

- унормування процедури обґрунтування доцільності, необхідності передачі секретної інформації іноземній стороні;

- визначення критеріїв проведення оцінки можливих політичних, правових, соціально-економічних, фінансових, гуманітарних та інших наслідків передачі секретної інформації іноземній стороні тощо.

Подальше нормативно-правове упорядкування питань пов'язаних з передачею державної таємниці України іноземній державі повинно сприяти зміцненню міждержавного авторитету та підвищення рівня безпеки України.

Література

1. Про державну таємницю: Закон України // Відомості Верховної Ради України (ВВР), 1994. - № 16. - Ст. 93.

2. Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації: Указ Президента України від 14 грудня 2004 року № 1483/2004. URL: https://zakon.rada.gov.ua/laws/show/1483/2004.

3. Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства: Указ Президента України від 17 липня 2006 року № 621/2006 URL: https://zakon.rada.gov.ua/laws/show/621/2006.

4. Гладківська О.В. Інформація з обмеженим доступом: проблема неузгодженості термінології // Інформація і право. – 2014. – № 1(10). – С. 49-58.

5. Щодо підготовки міжнародних договорів у сфері охорони інформації з обмеженим доступом. URL: https://ssu.gov.ua/ua/pages/172.

УДК 004.3.056(075)

Козюра В.Д.
кандидат технічних наук, доцент,
Національна академія Служби безпеки України
Степаненко В.І.
Державний університет телекомунікацій
Хорошко В.О.
доктор технічних наук, професор,
Національний авіаційний університет

СИСТЕМНИЙ ПІДХІД В ПРОЕКТУВАННІ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Проблема захисту критичних інформаційних інфраструктур від кіберзагроз зростає з кожним роком. Не дивлячись на те, що додаються колосальні зусилля в проектуванні і використанні високовартісних технічних засобів захисту, впровадженні строго регламентованих організаційних заходів, відповіді на найважливіше питання – наскільки запропоновані і реалізовані рішення дійсно хороші, яка їх планована і реальна ефективність - на жаль досі немає. Причина цього криється в [1, 2]:

- ігноруванні системного підходу до методології аналізу і синтезу побудови комплексних систем захисту інформації;
- відсутності механізмів повного і достовірного підтвердження якості КСЗІ;
- недоліках правового і нормативно-методичного забезпечення інформаційної безпеки, передусім в області визначення показників і критеріїв.

Застосування системного аналізу для вирішення завдань усіх етапів створення, впровадження і експлуатації КСЗІ дозволить забезпечити повноту і ефективність реалізацій їх функцій, а також оптимальні ресурсні, фінансові і тимчасові параметри для досягнення поставлених цілей [2, 3]:

- запобігання витоку, розкраданню, втраті, спотворенню, підробці інформації;
- запобігання загрозам безпеки особі, суспільству, державі;
- запобігання несанкціонованим діям зі знищення, модифікації, спотворення, копіювання, блокування інформації;

- запобігання іншим формам незаконного втручання в інформаційні ресурси і інформаційні системи, забезпечення правового режиму документованої інформації як об'єкту власності;

- захисту конституційних прав громадян на збереження особистої таємниці і конфіденційності персональних даних, наявних в інформаційних системах;

- збереження державної таємниці, конфіденційності документованої інформації відповідно до законодавства;

- забезпечення прав суб'єктів в інформаційних процесах і при розробці, виробництві і застосуванні інформаційно-телекомунікаційних систем, технологій і засобів їх забезпечення.

Проектування КСЗІ – це досить складний комплекс робіт, який зазвичай включає наступні етапи [4]:

1) формування загальних вимог до КСЗІ в ІТС;

2) розробка політики безпеки інформації в ІТС;

3) розробка технічного завдання на створення КСЗІ;

4) розробка проекту КСЗІ;

5) введення КСЗІ в дію та оцінка захищеності інформації в ІТС;

6) супроводження КСЗІ.

При проектуванні КСЗІ слід дотримуватися наступних принципів системного аналізу:

1. Принцип кінцевої мети – будь-яка спроба зміни складу або вдосконалення процедур використання програмних і апаратних компонент повинна оцінюватися відносно того, допомагає вона або заважає досягненню кінцевої мети. При цьому мета функціонування штучної системи задається, як правило, системою, в якій досліджувана система є складовою частиною.

2. Принцип виміру – оцінка ефективності проектованої КСЗІ повинна носити кількісний характер (навіть у разі, коли безліч показників носить якісний характер, є можливість перейти до кількісних оцінок, використовуючи такі теорії, як нечіткі множини або аналітичну ієрархію).

3. Принцип еквіфінальності – КСЗІ, яка проектується, повинна забезпечувати безпеку інформації, засобів інформації і захист інтересів учасників інформаційних стосунків і неможливість несанкціонованого доступу до інформації при різних станах зовнішнього середовища.

4. Принципам єдності – проектування підсистем і елементів КСЗІ необхідно орієнтувати на досягнення інтеграційного ефекту, щоб їх якісні і функціональні характеристики підвищували ефективність системи в цілому.

5. Принцип зв'язності – для проектування і ефективного управління КСЗІ у рамках організації необхідно розглядати її як підсистему. Безліч функцій КСЗІ при цьому знаходиться залежно від зв'язків організації із зовнішнім середовищем, з вищестоящими, нижчестоящими системами, а також внутрішніми зв'язками між структурними підсистемами.

6. Принцип модульної побудови дозволяє значною мірою абстрагуватися від надмірних деталей. Використання стандартизованих алгоритмічних і програмних рішень, засобів автоматизації і зв'язку, інших технічних елементів дозволяє понизити вартість і підвищити ефективність КСЗІ.

7. Принцип ієрархії – коли вводяться і поетапно розробляються різні рівні КСЗІ (організаційно-управлінські, технічні і т.д.).

8. Принцип функціональності – якщо існуюча організаційна, технологічна, управлінська, кадрова і т.д. структура системи не дозволяє забезпечити необхідні функціональні можливості, то така структура має бути змінена (перепроектована).

9. Принцип розвитку – можливість нарощування, модернізації, розширення якісних і функціональних характеристик КСЗІ**.**

10. Принцип децентралізації – раціональне поєднання елементів централізованого і децентралізованого управління КСЗІ.

11. Принцип невизначеності («людський чинник») – передбачити поведінку людини в різних ситуаціях повністю неможливо, проте спробувати мінімізувати можливий збиток в цьому випадку необхідно, і робити це слід ще на стадії проектування.

Висновки. Для забезпечення ефективності ІТС проектування КСЗІ доцільно базувати на наступних загальних принципах:

- вартість створення і експлуатації КСЗІ має бути менша, ніж розміри найбільш ймовірного або можливе допустимого збитку від будь-яких потенційних загроз;

- захист функціональних програм і даних має бути комплексним і багаторівневим, орієнтованим на усі види загроз з урахуванням їх небезпеки;

- КСЗІ повинна мати цільові, індивідуальні компоненти, призначені для забезпечення безпеки функціонування кожного окремо взятого об'єкту і функціонального завдання з урахуванням їх уразливості і ступені впливу на безпеку ІТС в цілому;

- КСЗІ не повинна призводити до відчутних труднощів, перешкод і зниження ефективності застосування і рішення основних функціональних завдань інформаційної системи в цілому.

Література

1. Андреев В.И. Проектирование систем технической защиты информации: учебное пособие / В.И.Андреев, Ю.Ю.Гончаренко, М.М.Дивизинюк, И.Н.Павлов, В.А.Хорошко. – Севастополь: Изд. Центр СНУЯЭиП, 2011. – 235 с.

2. Мамченко С.М. Комплексні системи захисту інформації: навчальний посібник / С.М.Мамченко, Козюра В.Д., Бровко В.Д. – К.: Нац. акад. СБУ, 2018. – 361 с.

3. Шумский А.А. Системный анализ в защите информации: учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности / А.А.Шумский, А.А.Шелупанов. – М.: Гелиос АРВ, 2005. – 224 с.

4. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

УДК 343.98
Корнейко О.В.
кандидат технічних наук, професор,
Національна академія внутрішніх справ
Школьніков В.І.
Національна академія внутрішніх справ

ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Компанія ThreatMetrix оприлюднила дані, що свідчать про збільшення обсягів кібератак на 30 % в Європі впродовж першого кварталу 2018 року [1]. Оскільки світ стає більш цифровим, кібератаки стають більш складними, то відповідно матеріально-технічне забезпечення правоохоронних органів повинно відповідати сучасним реаліям суспільного життя.

На жаль, слід відмітити недостатній рівень забезпечення правоохоронних органів відповідним комп'ютерним оснащенням.

Проблему недостатнього матеріально-технічного забезпечення можливо вирішити за допомогою використання хмарних технологій, обслуговування яких як правило є дешевшим порівняно із обслуговуванням традиційних персональних комп'ютерів.

Перевагами використання такої технології є:

– необов'язкова наявність потужних персональних комп'ютерів;

– економія витрат на використання ліцензованого програмного забезпечення та його постійного оновлення;

– великий обсяг пам'яті для зберігання даних;

– відсутність прив'язки до робочого місця, тобто існує можливість доступу до хмарних обчислень з різних пристроїв;

– високий рівень захисту даних та можливість відновлення інформації в разі її знищення.

Хмарні технології (з англ. Cloud Technology) – це нова інформаційна парадигма, що передбачає віддалену обробку та зберігання даних. Характерною ознакою цієї технології є використання електронно-обчислювальних можливостей віддалених серверів, які розташовані по всьому світові. Тобто, не обов'язково мати персональний комп'ютер із високими характеристиками процесора, оперативної пам'яті, відеокарти тощо. Головною умовою є наявність швидкісного підключення до Інтернету.

Необхідно погодитися із думкою Шепітька В.Ю. про те, що інформаційні технології надають можливість оперативного збирання, зіставлення та аналізу відомостей з різних джерел (повідомлень, результатів оперативно-розшукових заходів, допитів, адресної бази даних тощо), установлення хронологічної послідовності подій за часом та відповідності окремих фактів, дозволяють здійснювати складання планів та схем місця події, моделювання події злочину за допомогою комп'ютерної техніки та ін. [2, с. 196-197].

На сьогодні такі сервіси як Amazon Web Services та Digital Ocean Cloud Servers надають можливість використовувати віртуальні комп'ютери.

Наприклад, Amazon Web Services надає в оренду інфраструктуру для хмарних обчислень приватним або юридичним особам на основі платної підписки. Існує також і безкоштовна підписка, яка доступна протягом перших 12 місяців.

Ця технологія дозволяє мати в розпорядженні повноцінний віртуальний кластер комп'ютерів, який завжди доступний через Інтернет. Віртуальні комп'ютери AWS мають більшість атрибутів реального комп'ютера, включаючи апаратні пристрої (процесор, відеокарту, локальну та оперативну пам'ять, жорсткий диск або SSD-накопичувач); операційну систему на вибір; мережу; і попередньо встановлені прикладні програми тощо.

Слід відмітити, що AWS надає різні операційні системи у користування, починаючи від Windows 2016, Windows 2012 R та закінчуючи Ubuntu, CentOS, Red Hat Enterprise Linux.

Тобто, сервіс AWS може замінити традиційний персональний комп'ютер та бути використаним в діяльності правоохоронних органів, але відповідно до вимог чинного законодавства в сфері технічного захисту інформації та охорони державної таємниці.

Крім закордонних сервісів, правоохоронні органи мають можливість використовувати вітчизняні дата-центри, наприклад «Парковий».

Слід відмітити, що на разі в Верховній Раді України зареєстрований законопроект № 4302 від 24.03.2016 «Про внесення змін до деяких законів України (щодо обробки інформації в системах хмарних обчислень)», який передбачає використання органами державної влади хмарних технологій для обробки інформації (крім інформації, яка в установленому порядку віднесена до державної таємниці).

Сучасний розвиток інформаційних технологій надає правоохоронним органам безліч можливостей у боротьбі із злочинністю. Використання хмарних технологій можуть значно зекономити час та ресурси. Єдиною перепоною цьому є законодавче врегулювання можливості використання хмарних технологій під час обробки інформації, що становить державну таємницю. Це зумовлює необхідність подальших наукових розробок щодо можливості використання хмарних технологій в діяльності правоохоронних органів.

Література

1. 2018 Cybercrime Report Europe Deepdive. URL. [Електронний ресурс]. – Режим доступу: https://www.threatmetrix.com/info/2018-cybercrime-europe/ (дата звернення 04.03.2018).

2. Шепітько В.Ю. Інформаційні технології в криміналістиці та слідчій діяльності / В.Ю.Шепітько. Питання боротьби зі злочинністю. Харків, 2010. № 19. С. 194-202.

УДК 004.056.5
Корченко О.Г.
доктор технічних наук, професор,
Національний авіаційний університет
Дрейс Ю.О.
кандидат технічних наук, доцент,
Національний авіаційний університет

УДОСКОНАЛЕННЯ ІНСТИТУТУ ДЕРЖАВНИХ ЕКСПЕРТІВ З ПИТАНЬ ТАЄМНИЦЬ

На тлі посилення загроз і зростання нестабільності у світі через поширення недостовірної, неповної та упередженої інформації постають нові виклики національній безпеці в інформаційній сфері. Згідно Закону України "Про основи національної безпеки України" однією із реальних та потенційних загроз національній безпеці в інформаційній сфері є розголошення інформації, яка становить державну таємницю (ДТ), або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави [1].

З метою визначення та віднесення інформації до ДТ згідно з Законом України "Про державну таємницю" (далі – закон) [2] створено та функціонує в державі інститут державних експертів з питань таємниць (рис. 1).

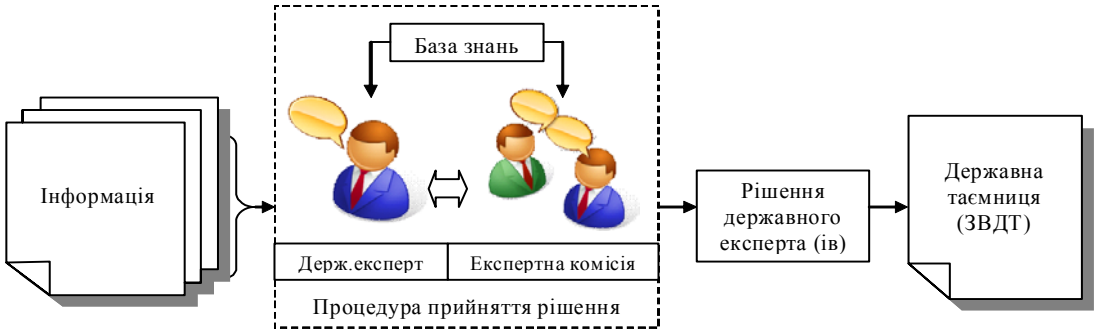


Рис.1. Проведення процедури прийняття рішення ДЕТ щодо віднесення інформації до ДТ

Державний експерт з питань таємниць (ДЕТ) – це посадова особа, уповноважена здійснювати відповідно до вимог цього Закону віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування [2]. ДЕТ несе персональну відповідальність за прийняті рішення. Згідно з чинним законодавством втручання будь-якої посадової особи, в тому числі тієї, якій підпорядкований державний експерт, до прийняття рішень з відне-

сення відомостей до ДТ неможливе. Такий порядок віднесення відомостей до ДТ забезпечує врахування сучасного рівня розвитку науки та техніки, результатів новітніх досліджень у відповідних наукових напрямках при проведенні роботи з віднесення відомостей до ДТ та забезпечує незалежність ДЕТ. При цьому Служба безпеки України, як спеціально уповноважений орган у сфері забезпечення охорони ДТ, забезпечує функціонування інституту ДЕТ та на підставі їх рішень формує Звід відомостей, що становлять державну таємницю (далі – ЗВДТ)[3, 4]. У працях вітчизняних авторів приділялася окрема увага до особливостей редакції [5], правового розвитку [6], питання необхідності категоризації та приведення змісту статей ЗВДТ до вимог законодавства тощо [7].

Відомо, що перелік посадових осіб, на яких покладається виконання функцій ДЕТ визначений Указом Президента України № 987/2009 (далі – Перелік). У 2010 році до цього Переліку входило 130, а наразі 145 посад. І, що цікаво, посада Президента України як Верховного головнокомандувача Збройних Сил України жодного разу не входила до цього Переліку, хоча згідно статті 5 закону [2], забезпечуючи національну безпеку, саме він видає укази та розпорядження з питань охорони ДТ.

Враховуючи те, що після подій 2014 року ряд посадових осіб, які також виконували функції ДЕТ, наразі або перебувають у розшуку, або отримали вирок суду про державну зраду, постає актуальне питання щодо необхідності удосконалення інституту ДЕТ у частині спрощення чи обмеження виконання окремих завдань ДЕТ визначених статтею 9 Закону [2] вищими політичними посадовим особами держави, або внесення змін до структури функціонування цього інституту, приділивши значну увагу до ролі експертних комісій при ДЕТ, адже більшу частину цих завдань виконують саме вони.

Автори також вважають, що для удосконалення інституту ДЕТ необхідно внести відповідні зміни до статей 8-12 Закону України “Про державну таємницю”.

Література

1. Ю. Дрейс, "Функціонування системи охорони державної таємниці в Україні: організаційно-правова структура, принципи та завдання", Безпека інформації, Т. 20. – № 2. – 2014. – С.176-184.

2. Про державну таємницю, Верховна Рада України; Закон від 21.01.1994 № 3855-XII {редакція від 05.08.2018}.

3. І. Божков, "Державна таємниця та система її охорони", Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – № 4. – 2002. – С.7-10.

4. О. Корченко, О. Архипов, Ю. Дрейс, "Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: монографія", К.: Наук.-вид. центр НА СБ України. – 332 с. – 2014. – ISBN 978-617-7092-26-0.

5. И. Божков, "Особенности новой редакции Свода сведений, которые составляют государственную тайну", Безопасность информации. – № 1. – 2001. – С. 4-5.

6. О. Корченко, Ю. Дрейс, "Правовий шлях формування зводу відомостей, що становлять державну таємницю", Проблеми створення, розвитку, застосування інформаційних систем спеціального призначення, ч.1: тези доп. 18-ї наук.-практ. конф., 15 квітня 2011, ЖВІ НАУ 2011. – С. 202-203.

7. О. Корченко, Ю. Дрейс, "Про необхідність категоризації та приведення змісту статей ЗВДТ до вимог чинного законодавства", Актуальні проблеми управління інформаційною безпекою держави: зб. мате VI наук.-практ. конф., 19 березня 2015 року, Київ, Наук.-вид. центр НА СБ України, 2015. – С. 270-273.

УДК 342.951:351

Коц Д.В.
начальник юридичного сектору
ІСЗЗІ Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

ПРАВОВІ ПИТАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Стрімкий розвиток сучасного інформаційного простору визначає необхідність створення правових підвалин інформаційної політики держави.

Проблема побудови світової системи захисту інформації пов’язана з появою першого інтернет-хробака Моріса у 1988 році в США. Саме тоді провідні фахівці з комп’ютерної безпеки зрозуміли необхідність комплексного підходу до забезпечення інформаційної безпеки та оголосили 30 листопада 1988 року Міжнародним днем захисту інформації [1]. Хробак Моріса вперше показав, наскільки небезпечно беззастережно довіряти комп’ютерним мережам, які потребують посилення та оновлення норм безпеки та захисту інформації.

Актуальність питання захисту інформації та її системи не викликає сумніву і тридцять років потому. 30 листопада 2018 року фахівці Державної служби спеціального зв’язку та захисту інформації України через офіційний веб-сайт Служби пропонували зробити декілька кроків для внеску в протидію ворогові [2] (як реальному так і евентуальному) та безпеки у кіберпросторі.

В українському законодавстві правові основи системи інформаційної безпеки сформульовані у статті 17 Конституції України, яка визначає інформаційну безпеку однією з найважливіших функцій держави, справою всього Українського народу [3].

Аналіз законодавчих актів показав, що у законодавстві України немає чіткого визначення терміну «система захисту інформації», проте його розуміння опосередковано містяться у низці інших законодавчо сформульо-

ваних понять. Ці поняття не є тотожними, однак дозволять нам сформувати власне розуміння системи захисту інформації.

Під системою технічного захисту інформації у частині першій статті 1 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» розуміється сукупність суб'єктів, що провадять діяльність у сфері технічного захисту інформації, нормативно-правових документів, що регулюють їх діяльність, а також матеріально-технічної бази у цій сфері [4]. На нашу думку, сучасні умови вимагають більш змістовного визначення поняття системи одного з видів захисту інформації.

Дослідження Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» виявило, що у статті 2 цього закону до об'єктів захисту в системі відноситься: 1) основний – інформація, що обробляється в цій системі, 2) додатковий – програмне забезпечення для обробки інформації [5].

Також наведемо законодавче розуміння національної системи кібербезпеки. Під такою системою у частині першій статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» розуміється сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури [6].

Як бачимо законодавець і в цьому випадку не включає до національної системи кібербезпеки об'єкти кібербезпеки і об'єкти кіберзахисту.

Такий підхід до формування понять системи не відповідає загальному уявленню про систему, адже системою є множина взаємопов'язаних елементів що утворюють єдине ціле, взаємодіють із середовищем та між собою.

Даючи розуміння поняттю системи захисту інформації, на нашу думку, не потрібно з її складу виключати об'єкти, на які впливають та/або щодо яких суб'єкти системи здійснюють свої повноваження, або, принаймні вказувати на мету/очікуваний результат роботи системи.

Аналогічне розуміння складових системи забезпечення інформаційної безпеки виразили Довгань О.Д. і Ткачук Т.Ю. у науковій праці «Система інформаційної безпеки України: онтологічні виміри»: «…основними елементами системи забезпечення інформаційної безпеки є її суб'єкти і об'єкти, а також прямі та зворотні зв'язки між ними.» [7, с. 93].

Формуючи власне розуміння поняття «система захисту інформації» органам, які здійснюються правозастосовну функцію, слід враховувати законодавчі визначення суміжних понять та не ігнорувати об'єкти щодо

яких здійснюються заходи захисту. Отже, на наш погляд, система захисту інформації це сукупність суб'єктів, що провадять діяльність із захисту інформації, об'єктів, щодо яких здійснюється захист, та взаємопов'язаних заходів науково-технічного, інформаційного, освітнього характеру, організаційних, правових заходів, а також інженерно-технічних засобів.

Висновок: проблема сучасного правового формулювання системи захисту інформації має важливе значення для розвитку інформаційної галузі. Використання системного підходу, як методу дослідження проблеми, буде сприяти розумінню розглянутого поняття, повній та всебічній розробці суб'єктами захисту інформації заходів досягнення мети (результату) та надасть можливість комплексно сприймати і оцінювати всі складові системи захисту інформації, зокрема з обмеженим доступом.

Література

1. Міжнародний день захисту інформації URL: https://uk.wikipedia.org /wiki/Міжнародний день захисту інформації (дата звернення 16.02.2019).

2. День захисту інформації: прості правила безпеки в кіберпросторі URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=300187&cat_id=284576 (дата звернення 16.02.2019).

3. Конституція України URL: zakon.rada.gov.ua/laws/show/254к/96-вр.

4. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» // Відомості Верховної Ради (ВВР), 2006, № 30, ст.258, № 3475-IV 23.02.2006.

5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» // Відомості Верховної Ради (ВВР), 1994, № 31, ст.286, № 80/94-ВР 05.07.1994.

6. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради (ВВР), 2017, № 45 ст. 403, № 2163-VIII 05.10.2017.

7. Система інформаційної безпеки України: онтологічні виміри / О. Довгань, Т. Ткачук // «Інформація і право». – 2018. – № 1 (24) – С. 89–103.

УДК 34.03+004+354

Кудінов В.А.
кандидат фізико-математичних наук, доцент,
Національна академія внутрішніх справ

УДОСКОНАЛЕННЯ НОРМАТИВНО-ПРАВОВОЇ БАЗИ У СФЕРІ ОХОРОНИ СЛУЖБОВОЇ ІНФОРМАЦІЇ ЄДИНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ

Останніми роками в Україні здійснюється реформа системи Міністерства внутрішніх справ (далі – МВС). Відповідно до Стратегії розвитку ор-

ганів системи МВС на період до 2020 року передбачено здійснити заходи щодо об'єднання і захисту інформаційних ресурсів органів системи МВС у межах єдиного інтегрованого інформаційного середовища [1]. Тому в МВС, на виконання Концепції програми інформатизації МВС на 2018-2020 роки [2], вживаються заходи щодо створення Єдиної інформаційної системи (далі – ЄІС).

ЄІС МВС – це багатофункціональна інтегрована автоматизована система, що становить сукупність взаємозв'язаних функціональних підсистем, програмно-інформаційних комплексів, програмно-технічних та технічних засобів телекомунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію [3]. Структура ЄІС складається з постійно діючих: центральної підсистеми; функціональних підсистем; транспортної мережі передачі даних; центрів обробки даних, телекомунікаційних мереж суб'єктів ЄІС; комплексних систем захисту інформації підсистем ЄІС з підтвердженою в установленому законодавством порядку відповідністю. Останні забезпечують захист інформації шляхом здійснення комплексу технічних, криптографічних, організаційних та інших заходів і використання засобів захисту інформації, спрямованих на недопущення блокування доступу до інформації, несанкціонованого ознайомлення з нею та/або її модифікації [3].

Відповідно до Переліку відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ України [4]: 1) у сфері інформаційних технологій службовою інформацією є інформація, що розкриває організацію, структуру, топологію, паролі доступу до централізованих обліків, баз (банків) даних та програмно-технічних комплексів, які входять до ЄІС МВС; 2) у сфері охорони інформації з обмеженим доступом службовою є інформація, що розкриває засоби та заходи захисту інформації на режимній території, в інформаційно-телекомунікаційних та комп'ютерних мережах тощо.

Власником і розпорядником ЄІС є держава в особі МВС. Володільцем інформації, що обробляється в центральній підсистемі ЄІС МВС, є МВС. Володільцями інформації, що обробляється у функціональних підсистемах ЄІС МВС, є відповідні суб'єкти ЄІС МВС (далі – ЦОВВ), які забезпечують захист інформації від випадкової втрати або знищення, незаконної обробки та незаконного доступу до інформації. Адміністратором ЄІС МВС є державне підприємство зі сфери управління МВС, яке забезпечує розроблення та здійснення заходів щодо захисту ЄІС та інформації, що міститься в ній [3]. На Департамент інформатизації МВС покладено завдання щодо організації роботи з проектування, створення, експлуатації та модернізації комплексних систем захисту інформації в інформаційних ресурсах ЄІС МВС [5].

Станом на сьогодні Перелік пріоритетних інформаційних ресурсів ЄІС МВС України містить 37 інформаційних ресурсів (Національна поліція – 18, МВС – 7, Адміністрація Держприкордонслужби – 5, Державна міграційна служба – 3, інші суб'єкти ЄІС – 4) [3]. При цьому мета обробки інформації у функціональних підсистемах ЄІС МВС установлюється нормативно-правовими актами, які регулюють діяльність відповідних ЦОВВ, окремо для кожного визначеного пріоритетного інформаційного ресурсу [3].

Таким чином, станом на сьогодні потребує удосконалення нормативно-правова база у сфері охорони службової інформації ЄІС МВС, зокрема, розроблення та прийняття в установленому порядку: 1) положень про відомчі інформаційні системи, бази (банки) даних; 2) порядку доступу користувачів до відомчих інформаційних ресурсів МВС та ЦОВВ, а також їх використання; 3) положення про комплексну систему захисту інформаційних ресурсів МВС та ЦОВВ, а також інших необхідних нормативно-правових актів.

Література

1. Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року : Розпорядження Кабінету Міністрів України від 15 лист. 2017 р. № 1023-р // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1023-2017-%D1%80/conv (дата звернення 06.03.2019).

2. Концепція програми інформатизації Міністерства внутрішніх справ на 2018-2020 роки, затверджена рішенням колегії МВС від 05 лист. 2018 р. № 18км : Наказ МВС України від 11 груд. 2018 р. № 1004.

3. Про затвердження Положення про Єдину інформаційну систему МВС та переліку її пріоритетних інформаційних ресурсів : Постанова Кабінету Міністрів України від 14 лист. 2018 р. № 1024. *Урядовий кур'єр* від 12 груд. 2018 р. № 235 // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF (дата звернення 06.03.2019).

4. Про затвердження Переліку відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ України : Наказ МВС України від 26 груд. 2016 р. № 1351 // База даних «Законодавство України» / *ЛІГА: ЗАКОН* : [сайт]. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/
MVS682.html (дата звернення 06.03.2019).

5. Про затвердження Положення про Департамент інформатизації Міністерства внутрішніх справ України : Наказ МВС України від 31 січ. 2018 р. № 70 // База даних «Законодавство України» / *ЛІГА: ЗАКОН* : [сайт]. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/MVS819.html (дата звернення 06.03.2019).

УДК 352/354.083.8:[316.77+070.13]
Муратов О.Є.
кандидат технічних наук,
старший науковий співробітник
Національна академія Служби безпеки України

ПЕРЕЛІКОВИЙ ТА БЕЗПЕРЕЛІКОВИЙ ПІДХОДИ ДО ЗАСЕКРЕЧУВАННЯ ІНФОРМАЦІЇ ТА ЇЇ МАТЕРІАЛЬНИХ НОСІЇВ

У Стратегії національної безпеки України, затвердженій Указом Президента України від 26 травня 2015 року № 287/2015, серед загроз кібербезпеці та безпеці інформаційних ресурсів зазначено фізичну і моральну застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [5]. Для удосконалення системи охорони державної таємниці в Україні та її підтримання у відповідності з вимогами сьогодення в Службі безпеки України було визначено напрями вдосконалення відповідного нормативно-правового забезпечення, зокрема такі: удосконалення механізму засекречування та розсекречування інформації, можливість упровадження стандартів та процедур НАТО та ЄС щодо визначення ступенів обмеження доступу (важливості) інформації [6].

Інститут державної таємниці в Україні в частині засекречування (розсекречування) інформації на момент свого утворення вже зазнав істотних змін порівняно зі своїм попередником, сформованим у колишньому СРСР, через позбавлення секретності своєї правової основи, передбачення підінституту державних експертів з питань таємниць і більш чітку регламентацію розсекречування інформації. Для подальшого вдосконалення сучасного інституту засекречування (розсекречування) інформації в Україні з урахуванням тенденцій включення до державних секретів службової інформації (див., наприклад, [6]) слід розрізняти два підходи, що виробила світова практика, до засекречування інформації та її матеріальних носіїв, на базі яких утворювався зазначений інститут в Україні.

Один із них – «переліковий» (цитовано за [2, с. 70]). Цей підхід вимагає визначати всю секретну інформацію в певних систематизованих каталогах-переліках. Для одержання відповіді на питання про секретність (несекретність) інформації на її матеріальному носії слід провести порівняння інформації, секретність якої оцінюється, з інформацією, наведеною в цих переліках. Гіпотетично будь-яка особа, яка має перелік, може перевірити належність певної інформації до секретної.

Інший підхід – можна назвати його «безпереліковий» – склався, наприклад, у правовій системі США [1]. За цим підходом визначаються сфери державного управління, де можливе засекречування інформації, і фактично будь-яка інформація із цих сфер може бути засекреченою на влас-

ний розсуд уповноваженою особою під час створення матеріального носія цієї інформації. У подальшому засекречуванню підлягають усі матеріальні носії інформації, де відтворюється інформація з уже засекреченого. За цим підходом тільки обмежена кількість визначених осіб може засекречувати (розсекречувати) інформацію та її матеріальні носії. Підхід не передбачає необхідності створення переліків усієї секретної інформації. Проте каталоги-переліки засекречених матеріальних носіїв інформації існують.

Підходи відрізняються способом формування елементів (понять), що становлять секретну інформацію. У переліковому підході загальний обсяг секретної інформації змінюється завдяки долученню або вилученню певних ознак-описів, найменувань елементів, з яких складається цей обсяг. У безпереліковому – обсяг секретної інформації змінюється завдяки прямому долученню або вилученню конкретних елементів без необхідності окремого визначення їхніх найменувань, ознак-описів, переліків тощо, які уточнюють властивості, що зумовлюють необхідність їхнього засекречування.

У зазначених підходах до формування масиву секретної інформації можна побачити певну аналогію з існуючими семантичними способами визначення відповідності (зв'язку) між поняттями (одиницями мови) і об'єктами із предметної області, які позначаються цими поняттями. За правилами семантики будь-яка така відповідність може бути визначеною [3]: екстенсіонально – шляхом прямого перелічення об'єктів, що складають обсяг поняття; інтенсіонально – шляхом визначення смислових ознак об'єктів, що називаються цим поняттям. Інтенсіональний спосіб уважається складнішим, проте він дає змогу точніше визначати відповідне поняттю коло об'єктів предметної області без їхнього прямого перерахування. Отже, раніше розглянуті два підходи до формування секретів – переліковий та безпереліковий – можна також називати відповідно інтенсіональним та екстенсіональним способами (підходами) формування масиву секретної інформації.

Сформований на сьогодні в Україні підхід до засекречування інформації можна вважати переліковим (інтенсіональним), який порівнянно з екстенсіональним (безпереліковим) є більш прийнятним для здійснення незалежного контролю, мінімізації кількості засекречених носіїв інформації, вчасного розсекречування інформації. Водночас, досягнення цих переваг сполучається з підвищеними витратами на етапі засекречування інформації через необхідність створення та підтримання функціональності відповідних переліків.

Література

1. Муратов О. Є., Ворожко В. П. Основні положення порядку засекречування інформації у США // Безпека інформації. 2012. № 1(17). С. 4–9.

2. Корченко О. Г., Архипов О. Є., Дрейс Ю. О. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: моногр. Київ: Національна академія СБ України, 2014. 332 с.

3. Попов Э. В. Общение с ЭВМ на естественном языке. Москва: Наука, 1982. 360 с.

4. Про державну таємницю: Закон України в редакції від 05.08.2018. URL: https:// zakon.rada.gov.ua/laws/show/3855-12 (дата звернення: 22.02.2019).

5. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: затв. Указом Президента України від 26 травня 2015 року № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення: 22.02.2019).

6. Семенюк О. Правова система охорони державної таємниці: історія становлення, сучасний стан, проблеми реформування // Юридична Україна. 2017. № 4. С. 58-66.

УДК 378.14

Самойленко О.О.
кандидат педагогічних наук
Кащук В.І.
Решетніков О.В.
Національна академія Служби безпеки України

ТЕСТУВАННЯ ЯК ЕЛЕМЕНТ ТЕХНОЛОГІЙ ДИСТАНЦІЙНОГО НАВЧАННЯ В ПРОЦЕСІ ПІДГОТОВКИ МАЙБУТНІХ БАКАЛАВРІВ З ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ

На сьогодні одним із пріоритетних завдань закладіввищої освіти є формування інформаційно діяльнісного простору, що сприятиме реалізації відповідних освітніх програм. Звідси, вибір методів, форм і засобів навчання повинен бути, у першу чергу, орієнтований на перехід від групових до індивідуальних, з власною особистісно орієнтованою траєкторією навчання.

Цілком логічним вбачається той факти, що до майбутніх бакалаврів з організації захисту інформації висуватиметься нова вимога уміння самостійно опрацьовувати та аналізувати великі масиви інформації, демонструючи при цьому відповідні програмні результати навчання у межах відповідної освітньо-професійної програми. Звідси, важливою ланкою освітнього процесу стає самеконтроль знань і умінь здобувачів вищої освіти.

Поступовий перехід від традиційних форм контролю і оцінювання знань до тестування у LMSMOODLE більш повно відповідає тенденціям модернізації та осучаснення вітчизняної системи освіти, діючим законодавчим та нормативно-правовим документам.

Розгортання єдиного інформаційного середовища професійної підготовки майбутніх бакалаврів з організації захисту інформації на основі LMSMOODLE (https://ppo.mk.ua/) уможливлює створення віртуального простору з необмеженими можливостями для комунікації, співпраці й кооперації учасників освітнього процесу, забезпечує взаємодію здобувача вищої освіти з викладачем або з програмними засобами, зокрема шляхом тестування. Так, тестування є ключовим елементом педагогічного контролю в сучасних навчальних електронно-освітніх комплексах [3, с. 51-52].

В педагогічній літературі поняття «тест» тлумачиться як сукупність завдань, яка дозволяє кількісно оцінити знання, вміння, навчальні досягнення, компетентність здобувачів вищої освіти [1, с. 902]. Критеріями якості тесту залишається його об'єктивність, надійність, валідність і складність. З огляду на це зазначимо, що LMSMOODLE дозволяє не лише регламентувати процедуру тестування, а й забезпечити оцінювання навчальних досягнень суб'єкта вимірювання із дотриманням критеріальних вимог до якості тесту.В процесі професійної підготовки майбутніх бакалаврів з організації захисту інформації із використанням LMSMOODLE тестування, як правило, проводиться в оф-лайновій формі, що обґрунтовується наступним: вказана форма не «прив'язує» учасників освітнього процесу до конкретного моменту часу. Крім того, програмні ресурси LMSMOODLE дозволяють створювати різні типи тестів для перевірки якості знань [2].

Оцінка виставляється як автоматично, так і викладачем (за умови наявності в тесті відкритих питань). Час кожної відповіді у тесті обмежений (не надана вчасно відповідь на питання змінюється наступним питанням). Час відправки тесту також фіксується. Часовий критерій є важливим і його слід чітко дотримуватися. Це, у свою чергу, сприятиме формуванню у здобувачів вищої освіти не лише фахових (спеціалізованих) компетентностей, а й здатності ефективно управляти часом. Довжина модульного тесту становить 10-20 тестових завдань, а підсумкового тесту 50-60 тестових завдань.

Вважаємо за необхідне зазначити, що ресурс «Тест» в LMSMOODLE дозволяє фіксувати, зберігати отримані відповіді, реєструвати час надходження відповідей, встановити зворотній зв'язок із здобувачами вищої освіти, зосередити увагу учасників освітнього процесу на прогалинах у знаннях і вміннях і, відповідно, внести корективи.

Підсумовуючи, слід зазначити, що тестування у LMSMOODLE як форма контролю знань здатне забезпечити:безпечне досягнення дидактичних цілей;розширення діапазону інформаційних потреб;об'єктивність та прозорість моніторингу якості освіти;усунення територіальних та часових бар'єрів в освітньому процесі;мотивовану самостійну роботу здобувачів вищої освіти у процесі оволодіння професією;автоматизацію процесів організації й управління особистісно орієнтованою траєкторією навчання.

Проведене дослідження не вичерпує всіх аспектів зазначеної проблеми. Перспективою подальших досліджень є вивчення світових інноваційних тенденцій у напрямі підвищення якості тестування у LMSMOODLE як інструменту виявлення якості знань і вмінь здобувачів вищої освіти.

Література

1. Енциклопедія освіти / Акад. пед. наук України; головний ред. В.Г. Кремень. К: Юрінком Інтер, 2008. 1040 с.

2. Самойленко О.М. Впровадження технології персонального навчального вебресурсу викладача в університетську освіту [навч.-метод. посіб.] / О.М. Самойленко, В.Д. Будак, В.В. Олійник, Н.С. Ручинська. Миколаїв : МНУ, 2013. 156 с.

3. Технологія роботи в єдиному інформаційному середовищі на основі Office 365: зб. матеріалів методологічного семінару 18 травня 2017 р. [ред. кол.: В.В. Олійник (голов. ред.) та ін.]. К.: ДВНЗ «Ун-т менеджменту освіти» НАПН України, 2017. 116 с.

УДК 65.012.8 (477)

Сидоренко С.М.
Національна академія Служби безпеки України

ХАРАКТЕРИСТИКА ДЕРЖАВНО-ПРАВОВИХ МЕХАНІЗМІВ РЕСПУБЛІКИ ЛИТВИ У СФЕРІ БЕЗПЕКИ СЕКРЕТНОЇ ІНФОРМАЦІЇ

Політика в області захисту секретної інформації формується Урядом Республіки Литви та Комісією з координування захисту таємниць країни. Заходи у сфері безпеки секретної інформації здійснюють Уряд РеспублікиЛитви, Комісія з координування захисту таємниць,Служба нагляду за безпекою країни, Національна служба по захисту комунікацій, Національна служба розподілу шифрів.

Відповідальність за безпеку секретної інформації на підприємствах, установах і організаціях, у яких зберігається або використовується секретна інформація, несуть їх керівники, уповноважені ними особи, а також особи, яким ця інформація довірена. Пряму відповідальність за втрату або незаконне розголошування довіреної секретної інформації несе особа, якій така інформація довірена.

У структурних підрозділах, які мають у своєму розпорядженні інформацію, що становить державну таємницю Литовської Республіки, в обов'язковому порядку формуютьсясписки осіб, яким видані дозволи на проведення секретних робіт та ознайомлення із секретною інформацією.

Захист секретної інформації координують створювані рішенням керівника постійні спеціальні експертні комісії. Вони:

1) розробляють правові акти, пов'язані із захистом секретної інформації, здійснюють нагляд за виконанням цих правових актів;

2) представляють пропозиції керівникові щодо видачі особам дозволів на проведення робіт та на ознайомлення із секретною інформацією, або відміни виданих дозволів;

3) представляють висновки і пропозиції щодо обгрунтованості засекречування інформації, зміни грифів секретності, розсекречення або знищення секретної інформації;

4) організовують перевірки стану секретної інформації, яку має у своєму розпорядженні суб'єкт таємниць, і вносять пропозиції щодо превенції порушення вимог по захисту секретної інформації, вирішують інші питання, пов'язані із захистом секретної інформації.

Заходи з безпеки інформації Республіки Литви із грифами секретності «Цілком таємно», «Таємно» і «Конфіденційно», або передану Литовській Республіці інформації, що складає таємницю інших держав або міжнародних організацій, в органах Республіки Литви координуються колегіальним органом країни – Комісією з координування захисту таємниць. Положення про Комісію з координування захисту таємниць затверджується Урядом РеспублікиЛитви.

До складу Комісії з координування захисту таємниць входять сім членів – по два представники делегують Президент Республіки, Голова Сейму, Прем'єр-міністр країни. Головою комісії є генеральний директор Департаменту державної безпеки.

Функції секретаріату Комісії з координування захисту таємниць виконує структурний підрозділ Департаменту державної безпеки.Керівник підрозділу призначається секретарем Комісії з координування захисту таємниць. Секретаріат Комісії з координування захисту таємниць готує матеріали засідань Комісії, контролює виконання прийнятих рішень суб'єктами таємниць.

Література

1. Конституція Республіки Литви. 25 жовтня 1992 р. http://www3.lrs.lt/home/Konstitucija/Constitution.htm.

2. Закон Республіки Литви "Про державні і службові таємниці". № VIII – 1443, 25 листопада 1999 р. (із змінами і доповненнями від 20 листопада 2001 р. № IX - 613). http://www3.lrs.lt/cgi-bin/getfmt?c1=w&c2=157736. Див. НАТО, Основна інформація про національну програму інтеграції Литви в НАТО, 1999-2000 р. http://www.nato.int/pfp/lt/current/ANP/anp2000.html.

3. Закон Республіки Литви "Про надання інформації громадськості". 2 липня 1996 р. № I-1418 (із змінами і доповненнями від 20 червня 2002 р. № IX–972). http://www3.lrs.lt/cgi-bin/getfmt?c1=w&c2=170831.

4. № X-383 від 10 листопада 2005 р. Див. ЄС, Статус виконання Директиви про державну інформацію. http://europa.eu.int/information_society/policy/psi/implementation/status/index_en.htm.

5. Звіт за оцінкою Литви 4-8 березня 2002 р. GrecoEval I Rep (2002) 1E Final. Комітет GRECO, перший етап оцінки.

УДК: 338.483.15
Чередниченко О. Ю.
доктор філософії в галузі економіки, доцент,
Інститут підготовки юридичних кадрів для СБ України
Національного юридичного університету ім. Ярослава Мудрого
Козлова А.О.
кандидат економічних наук,
Харківський національний університет
міського господарства імені О.М. Бекетова

ПРОБЛЕМНІ ПИТАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН, ЩО ВИКОРИСТОВУЮТЬСЯ В ТУРИСТИЧНИХ УСТАНОВАХ

Туристична галузь, незважаючи на певні кризові явища в економіці держави, має величезний потенціал та перспективи до розвитку, що робить її досить привабливою як для туристів чи туристичних установ так і державних інституцій.

Аналіз попиту на туристичному ринку свідчить про те що турист при виборі тура перше на що звертає увагу так це на його ціну, рівень сервісу, трансферні послуги, привабливість екскурсійної програми. При цьому, безпека туристів для наших співвітчизників є традиційно не першочерговою умовою. Доречи питання забезпечення безпеки туриста починається ще на стадії оформлення документів в туристичній агенції. Туристи надають менеджерам туристичних установ копії закордонних паспортів, іншу інформацію що містить особисті дані, що охороняються законом України «Про захист персональних даних». При цьому в більшості туристичних агенціях та установах взагалі відсутня система захисту персональних даних туристів.

Так, клієнту, як правило, не доводяться вимоги закону України «Про захист персональних даних», не отримується письмова згода на використання його персональних (особистих) даних, а сама конфіденційна інформація зберігається, обробляється та використовується з явними порушеннями діючого законодавства. Відповідно до технології роботи туристичних установ після отримання вказаної інформації у туристів безпосередньо туристичними агенціями їх персональні дані передаються туристичним операторам та готельєрам.

Передача вказаних даних здійснюється засобами мережі Інтернет, а також за допомогою електронної пошти, факсимільного зв'язку та інших відкритих (незахищених) каналів зв'язку.

На протязі всього туру персональні дані туристів використовуються також страховими установами, авіакомпаніями, установами які надають послуги з трансферу, готельними менеджерами, менеджерами з продажу і організації екскурсійного продукту тощо. Яким чином при цьому забезпечується охорона персональних даних туристів теж не відомо. Крім того,

перебування туриста за межами нашої держави нівелює вимоги норм закону України «Про захист персональних даних» взагалі.

Таким чином, виникають передумови до безконтрольного, несанкціонованого доступу та використання персональних даних туристів, в тому числі з боку як злочинних угрупувань (наприклад різного роду шахраїв, торгівців людьми, піратів, наркоторговців), так і окремих осіб чи організацій терористичної спрямованості, або представників незаконних воєнізованих, іноземних спецслужб.

При цьому більшість туристів та туристичного менеджменту навіть не уявляють небезпечні наслідки вищенаведеного, бо традиційно вважається що захистом громадян повинні опікуватися державні органи та правоохоронці країни перебування.

Нашу думку важливим є те, що туристичні оператори, менеджмент туристичних агенцій та структур які з ними співпрацюють теж повинні активніше «включатися» в цю роботу. Мова йдеться, перш з все, про дії які не потребують значних додаткових фінансових затрат, а саме про:

- роз'яснювально-профілактичну роботу з клієнтами-туристами (наприклад: доведення туристу при придбанні туру норм законодавства про захист його персональних даних, правил безпеки в конкретній країні, надання інформації про поведінку у разі потрапляння у надзвичайну ситуацію та контакти органів влади, правоохоронців тощо);
- взяття на себе письмових зобов'язань щодо захисту персональних даних туриста та відображення це в договорі на туристичні послуги;
- забезпечення умов зберігання, обробки та використання персональних даних та іншої конфіденційної інформації відповідно до норм діючого законодавства;
- забезпечення захищеності каналів при передачі персональних даних та іншої конфіденційної інформації та недопущення при цьому неконтрольованого витоку вказаної інформації;
- запровадження захисту комп'ютерних мереж туристичних установ від «хакерських» атак та шкідливих вірусних програм;
- пошук форм більш плідної взаємодії між туристичними установами і органами влади, правоохоронцями (наприклад, на рівні консульських структур міністерства закордонних справ, щодо недопущення неконтрольованого обігу інформації про громадян України в країні їх перебування) тощо.

Ще однією важливою умовою, яка дозволить на нашу думку мінімізувати негативні наслідки, є контроль з боку уповноважених державних інституцій щодо дотримання законодавства про захист конфіденційної та службової інформації в туристичному секторі.

Крім того, дуже важливою умовою є надання допомоги цими державними інституціями допомоги туристичним установам щодо організації, налагодження та функціонування системи захисту вказаної інформації та вищенаведених превентивних заходів.

АКТУАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ ТА ШЛЯХИ ЇЇ УДОСКОНАЛЕННЯ

УДК 316.422
Автушенко О.С.
кандидат педагогічних наук, доцент
Кожедуб Ю.В.
кандидат технічних наук
ІСЗЗІ «КПІ ім. Ігоря Сікорського»

ПРОБЛЕМНІ ПИТАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Проблема кіберзлочинності, на сучасному етапі історичного розвитку, набуває глобального виміру та становить загрозу інформаційному суспільству. У процесі свого формування поняття «кіберзлочинність» пройшло низку етапів та отримало відображення у нормативно-правових актах національного та міжнародного рівнів.

Боротьба з кіберзлочинністю потребує активного та тісного міжнародного співробітництва усіх сучасних держав. Одним з таких кроків є підписання у листопаді 2001 року Радою Європи, а також США, Канадою та Японією «Конвенції про кіберзлочинність» [1]. Перспективою подолання проблеми кіберзлочинності може стати подальше поглиблення співпраці держав та міжнародних інститутів у виявленні, а головне попередженні ймовірних кіберзагроз.

Розглядаючи протидію злочинам у сфері використання комп'ютерних технологій, з точки зору міжнародного співробітництва, слід зрозуміти причини їх підвищеної небезпеки для світового співтовариства та виокремити основні проблеми, що зумовлено певними особливостями, властивими саме цьому різновиду злочинності, а саме: міжнародний характер – тобто, у злочинця є можливість несанкціоновано проникнути в будь-яку комп'ютерну систему, яка з'єднана зі світовою мережею Інтернет (незважаючи на державні кордони та відстань до неї); високий рівень латентності, причинами якого є: складність практичного виявлення злочинів правоохоронними органами; небажання потерпілих повідомляти про вчинений проти неї злочин; помилкове (чи умисне) «списання» наслідків протиправних посягань за рахунок апаратно-програмних проблем комп'ютерних систем; недостатність стандартизованих методик розкриття та розслідування вказаних злочинів, налагоджених механізмів міждержавної взаємодії в розслідуванні; значний рівень залежності

сучасного суспільства від інформаційних технологій, які охоплюють майже всі сфери життєдіяльності людини та функціонування держави (банківська, енергетична, транспортна, оборонна та інші сфери), і можуть розглядатися як потенційні об'єкти кібератак.

Аналіз системи кібернетичної безпеки провідних країн вказує на такі основні тенденції у цій сфері, як: відповідна системна реорганізація сектору безпеки та створення спеціалізованих підрозділів із захисту національних інтересів у кіберпросторі.

Існує ціла низка проблем щодо побудови національної системи кібернетичної безпеки, з поміж яких можна виділити такі:

відсутність як для державного, так і для приватного сектору стандартів кібернетичної безпеки на основі визнаних міжнародних стандартів;

незавершеність нормативно-правового регулювання процесу розбудови системи кібернетичної безпеки України;

необхідність удосконалення національного законодавства щодо спрощення процедур міжнародного співробітництва при реагуванні на кіберінциденти;

відсутність чіткого розподілу функцій між суб'єктами забезпечення кібернетичної безпеки та їх повноважень.

У зв'язку з цим важливе значення має затвердження Стратегії кібербезпеки України Указом Президента України від 15 березня 2016 року [3], основною метою якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Для досягнення поставленої мети необхідно:

створити національну систему кібербезпеки;

посилити спроможності суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглибити міжнародне співробітництво у цій сфері;

забезпечити кіберзахист державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України.

Також своєчасним та необхідним є прийняття Закону України від 5 жовтня 2017 року № 2163-VIII «Про основні засади кібербезпеки України» [2] у якому визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та гро-

мадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Отже, на сьогоднішній день, в Україні створено умови для боротьби з кіберзлочинністю, визначено цілі, напрями та принципи державної політики у сфері кібербезпеки, затверджено Стратегію кібербезпеки України, основною метою якої є створення умов для безпечного функціонування кіберпростору. Все це дає нам сподівання на розв'язання проблем забезпечення кібернетичної безпеки держави.

Література

1. Конвенція про кіберзлочинність // Офіційний вісник України – 2007. – № 65. – Ст. 2535. – С. 107.
2. Про основні засади кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII // Відомості Верховної Ради. – 2017. – № 45. – Ст. 403.
3. Стратегія кібербезпеки України: Указ Президента України від 15 березня 2016 року № 96/2016 // Урядовий кур'єр. – № 52.

УДК 35.078.3

Алексєєв М.М.
Національний університет оборони України
імені Івана Черняховського

УПРАВЛІННЯ РИЗИКАМИ У СФЕРІ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ: СТРУКТУРОВАНИЙ ІТЕРАЦІЙНИЙ ПІДХІД

Автоматизація, розповсюдження та постійне удосконалення механізмів кібернетичних атак все більше підштовхують фахівців у сфері кібернетичної безпеки до застосування технологій управління ризиками, де *ризик* визначається як наявність загрози, пов'язаною з існуючою вразливістю, що може завдати шкоди певному активу.

Управління ризиками - це безперервний, ітеративний та еволюційний процес. Кожна ітерація поділяється на три етапи: визначення ризиків; зменшення ризиків; оцінка ризиків.

В рамках першого етапу визначається ризик та його компоненти, такі як загрози, вразливості та його ймовірність в межах чітко визначеної сфери, тобто здійснюється ідентифікація ризику. Далі аналізується його вплив. Тобто метою визначення ризику є формування його повного опису та оцінка його важливості на основі визначених імперативів (характеризація ризику).

Розглянемо приклад із сфери кібернетичної безпеки (КБ): сканування вразливості (Penetration test) - тест на проникнення, який є інструментом для ідентифікації та аналізу недоліків кібернетичної системи (КС), що

можуть бути використані для шкідливої атаки на певний об'єкт кібрезахисту. Для того, щоб визначити, чи дійсно така вразливість становить проблему для вказаного об'єкту здійснюється оцінка ступеню її негативного впливу на конкретний об'єкт. Цей процес дозволяє з'ясувати результати сканування в контексті визначеної організації.

На даному етапі зазвичай використовується структурований ітераційний підхід, який визначається загальним набором термінів та системних показників.

На наступному етапи, враховуючи можливий вплив визначених ризиків, приймається рішення щодо конкретної політики стосовно кожного з них. За своєю природою такі заходи можуть бути юридичними або адміністративними, організаційними або процедурними, або програмно-технічними методами [1].

З цього моменту починається фаза зменшення ризиків – етап під час якого дуже важливо здійснити правильне визначення пріоритетів та раціонально розподілити наявні ресурси. Головною метою фази зменшення ризиків є планування та реалізація заходів, спрямованих на протидію визначеним ризикам або контроль за ними, зазвичай, на основі економічної ефективності.

Після імплементації запланованих заходів починається фаза оцінки ризиків, яка полягає в постійному моніторингу визначеного ризику та аналізі ефективності вжитих заходів. Якщо ризик зменшується до визначеного припустимого рівня, захід вважається ефективним. В іншому випадку, або в разі появи нового ризику, запускається новий управлінський цикл з його першого етапу – визначення ризиків.

При цьому, на відміну від реактивного (подія – реакція) підходу, який застосовувався в минулому (наприклад: у разі зараження комп'ютера вірусом необхідно було вжити низку термінових заходів: по-перше, обмежити шкоду, по-друге, оцінити збитки, далі, визначити причину та усунути їх в подальшому шляхом оновлення політики чи процедури) сьогодні часто використовується проактивний (упереджу вальний) режим, коли з'являється час для завчасної, обґрунтованої та раціональної відповіді на можливі кіберзагрози для визначеної КС, або, в ідеалі, взагалі усуваються передумови до їх виникнення.

Проактивний режим перш за все передбачає підготовку плану реагування на виникнення ймовірних надзвичайних ситуації, своєчасну та регулярну перевірку конфігурації системи, визначення рівня оновлення програмного продукту, з'ясування ефективності системних і програмних обмежень від несанкціонованого доступу до самої КС та її ресурсів, проведення аудиту системних та мережевих журнальних записів (логів).

Такий алгоритм роботи, у більшості ситуацій, дозволить своєчасно викрити місце виникнення можливої кібератаки та з'ясувати ресурси, які

зазнали ураження. Після чого для поновлення нормального режиму функціонування відповідної КС вживаються заходи, визначені у завчасно розробленому плані реагування на надзвичайні ситуації.

Література

1. Гаценко С.С., Костянюк В.О. Джерела загроз інформаційній безпеці / Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів наук.-практ. конф. (Київ, 20 березня 2014 р) : у 2 ч. Ч. 1. – Центр навч.-наук. та наук.-практ.вид. НА СБ України, 2014.

2. NISTIR 7298 Revision 2: Glossary of Key Information Security Terms URL:https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

3. NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments URL:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

УДК 004.056:5:378.1(045)

Бровко В.Д.
кандидат технічних наук
Решетніков О.В.
Національна академія СБ України

ОРІЄНТОВНІ НАПРЯМИ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ДЛЯ ПОТРЕБ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Аналізуючи зазначені у Законі України «Про основні засади забезпечення кібербезпеки України» завдання суб'єктів забезпечення кібербезпеки можна дійти висновку про те, що у підготовці фахівців для національної системи кібербезпеки викреслюються декілька профілів:

1. Розвиток безпечного, стабільного і надійного кіберпростору як середовища (віртуального простору), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утвореного в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

2. Забезпечення захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

3. Забезпечення кіберзахисту державних електронних інформаційних ресурсів та об'єктів критичної інфраструктури на основі сукупності організаційних, правових, інженерно-технічних заходів, заходів криптографіч-

ного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем, а також створення автоматизованих систем управління інформаційною безпекою.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» Служба безпеки України повинна здійснювати запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснювати контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряти готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіяти кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідувати кіберінциденти та кібератаки щодо державних інформаційних ресурсів. Інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечувати реагування на кіберінциденти у сфері державної безпеки [1].

Для виконання вищезазначених завдань Службі безпеки необхідні фахівці у сфері кібербезпеки.

У цих тезах автори пропонують перелік спеціалізацій для підготовки професіоналів для національної системи кібербезпеки відповідно завдань, що стоять перед Службою безпеки України:

Організація протиборства та спеціальних операцій у кіберпросторі;

Організація розвідувальної та контррозвідувальної діяльності у кіберпросторі;

Організація контррозвідувальної та оперативно-розшукові діяльність у кіберпросторі;

Організація антитерористичної діяльності в кіберпросторі;

Організація розкриття кіберзлочинів спрямованих проти національної безпеки.

Організація та контроль кіберзахисту електронних інформаційних ресурсів;

Організація та контроль кіберзахисту об'єктів критичної інфраструктури.

Література

1. Закон України Про основні засади забезпечення кібербезпеки України // (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/2163-19.

УДК 519.816
Бутвін Б.Л.
доктор технічних наук, професор,
ЦНДІ ЗС України
Штифурак Ю.М.
кандидат технічних наук,
старший викладач
НТУУ “КПІ ім. Ігоря Сікорського”
Сидоренко О. В.
аспірант

МЕТОДИКА ОЦІНЮВАННЯ ІНТЕГРАЛЬНОГО РІВНЯ ЗАГРОЗ КІБЕРБЕЗПЕЦІ ДЕРЖАВИ

Одним із завдань виявлення більш небезпечних кібератак є розроблення методики їх оцінювання. Для детального оцінювання інтегрального рівня кіберзагроз розроблено методичний підхід на основі нелінійного, багатопараметричного методу оцінювання. Його реалізовано в програмному середовищі AnyLogic_8 [1, 4]. Для оперативного оцінювання індексу інтегрального рівня загроз кібербезпеці застосовано таку мультипликативну згортку [5]:

$$К_{з} = \frac{ЕЗ_{з}}{5} \cdot \frac{Х_{з}}{4} \cdot \frac{(\sum_{i=1}^{5} НЗ_{i})}{25} \qquad (1)$$

де : $К_З$ – інтегральний індекс (рівень) кіберзагрози (від 0 до 1), $ЕР_З$ – показник етапу розвитку кіберзагрози (від 1 до 5: 1 – зародження загрози, 2 – розвиток, 3 – загострення, 4 – відкрита атака, 5 – масова кібератака), $Х_З$ – показник масштабу кіберзагрози (від 1 до 4: 1 – локальна, 2 – загальнодержавна, 3 – регіональна, 4 – глобальна), $НЗ_1$, $НЗ_2$, $НЗ_3$, $НЗ_4$, $НЗ_5$ – показники прогнозованих наслідків кібератаки для життєво важливих інтересів України (від 0 до 5 за кожним показником: 0 – відсутні, 1 – незначні, 2 – середні, 3 – значні, 4 – руйнівні, 5 – катастрофічні).

Рейтингування кіберзагроз відповідно до отриманого індексу можливе на такі кластери:

1) загрози з високим рівнем ризику (потребують ужиття невідкладних заходів);

2) загрози із середнім рівнем ризику (потребують розроблення контрзаходів);

3) загрози з низьким рівнем ризику (потребують моніторингу).

Розподіл індексу загроз доцільно виконувати за такими інтервалами: 0-0,18 – низький рівень, 0,18-0,35 – середній рівень, 0,35-1 – високий рівень.

Слід відзначити, що для оцінювання показників EP_3, X_3, $НЗ_1$, $НЗ_2$, $НЗ_3$, $НЗ_4$, $НЗ_5$ застосовуються експертно-аналітичні методи. Принциповим положенням для їх застосування слід вважати відбір експертів з високим рівнем компетентності в заданій сфері кібербезпеки. Для його оцінювання доцільно застосовувати метод парних порівнянь як зворотносиметричної матриці методу парних порівнянь, розроблений Сааті [5].

Цей метод засновано на розрахунку чисельного значення показника узгодженості, що називається відношенням узгодженості (*ВУ*).

$$ВУ = \frac{IS}{SS}, \quad (2)$$

де *IS* – індекс узгодженості експертних оцінок, *SS* – випадкова узгодженість експертних оцінок матриці розмірністю $n \times n$ [5].

Показник *ВУ* характеризує узгодженість безлічі суб'єктивних оцінок, отриманих способом парного порівняння і представлених як відношення переваги порівнюваних властивостей.

Значення *ВУ*, менше або рівніше 0,1 (10%), вважається допустимим, а за початковими даними можуть бути отримані рішення. Якщо значення *ВУ* перевищує допустимий рівень ($ВУ_{доп} > 0,1$), то початкова інформація не достовірна.

Індекс узгодженості визначається за формулою:

$$SS = \frac{\lambda_{max} - n}{n - 1}, \quad (3)$$

де λ_{max} – найбільше власне значення матриці парних порівнянь, *n* – кількість стовпців і рядків матриці.

Найбільше власне значення визначається за формулами:

$$\lambda_{max} = R_1 \sum_{i=1}^{n} W_{i1} + R_2 \sum_{i=1}^{n} W_{i2} + R_i \sum_{i=1}^{n} W_{ij} + ... R_n \sum_{i=1}^{n} W_{in} \quad (4)$$

$$R = \sqrt[n]{\prod_{j=1}^{n} W_{ij}} \times \left\{ \sum_{i=1}^{n} \sqrt[n]{\prod_{j=1}^{n} W_{ij}} \right\}^{-1}, \quad (5)$$

де *i* – індекс рядка матриці М, *j* – індекс стовпця матриці М, w_{ij} – експертні оцінки.

Уведемо інтегральний показник компетентності експерта K_k^{ij} з урахуванням формул (2) – (5).

$$K_k^{ij} = \left\{ 1 - \frac{n_j (\lambda_{max} - n_j)}{2(n_j - 2)(n_j - 1)} \right\}, \quad (6)$$

де n_j – кількість часткових загроз у *j*-й сфері, λ_{max} – статистичний показник, який ураховує кількість порушень кардинальної транзитивності експертних оцінок та розраховується за формулою (5).

Отже, наведена вище методика дає змогу оцінити інтегральний рівень кіберзагроз з урахуванням розвитку та масштабності кіберзагрози, а також показників прогнозованих наслідків кібератаки для життєво важливих інтересів України.

Література

1. Бутвін Б.Л. Методичний підхід до визначення інтегрального рівня зовнішніх загроз кібербезпеці держави на основі нелінійного, параметричного методу їх оцінювання / Б.Л. Бутвін, Ю.М. Штифурак // Збірник наукових праць Інституту СЗР України. – 2018. – № 16 – С. 64-69.

2. Штифурак Ю.М. Методичний підхід до оцінювання стабільності держави (регіону) на основі нечітких когнітивних моделей / Ю.М. Штифурак // Збірник наукових праць Інституту СЗР України. – 2013. – № 6 – С. 91-99.

3. Бутвін Б.Л. Аналітична методика оцінки стабільності держави (регіону) / Б.Л. Бутвін, Ю.М. Штифурак // Збірник наукових праць Інституту СЗР України. – 2012. – № 3 – С. 132-139.

4. AnyLogic [Електронний ресурс] – Режим доступу : http://www.anylogic.ru/overview.

5. Саати Т. Л. Принятие решений / Т. Л. Саати. – М. : Радио и связь, 1993. – 278 с.

УДК: 378.016:004.056.5

Воскобойніков С.О.
кандидат педагогічних наук
Кащук В.І.
Решетніков О.В.
Національна академія Служби безпеки України

ФОРМУВАННЯ ФАХОВИХ КОМПЕТЕНЦІЙ КІБЕРЗАХИСТУ ДЕРЖАВНИХ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ПРОЦЕСІ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасні етапи розвитку інформаційних і комунікаційних технологій спричинюють поглиблену системну інтеграцію в інформаційному та кібернетичному просторі суспільства і держави. На думку фахівців і науковців Д. С. Бірюкова, С. І. Кондратова, Рогова П.Д., Воровича Б.О. Ворони Т.О. Бочкова А. [1, 2, 3 5], інформаційна сфера поступово стає важливим та значущим елементом яких потребує забезпеченні постійного захисту та безперервного функціонування в системі національної безпеки.

Означена потреба зумовлена забезпеченням безперервної діяльності таких об’єктів та кваліфікованих фахівців, які здійснюють кіберзахист інформаційних ресурсів та робота яких пов’язана із розв’язанням нових задач - реалізації захищених інформаційних потоків та унеможливлення по-

рушення сталого функціонування об'єкта критичної інфраструктури через здійснені на них кібератаки та кіберінциденти [4].

Впровадження інформаційних систем в процеси автоматизації управління державними процесами створює нові інформаційні потоки, які формують комп'ютерні мережі та телекомунікації, спричинює нові загрози для державних електронних інформаційних ресурсів.

На сьогоднішній день в правовому полі питання вимог до об'єктів критичної інфраструктури не конкретизовані, водночас немає переліку об'єктів критичної інформаційної інфраструктури.

Нормативно-законодавчим підґрунтям визначено, що галузь інформаційної і кібернетичної безпеки включає в себе правовий, організаційний, технічний і правоохоронний складники, стосується інформаційно-технологічного та інформаційно-психологічного протиборства. При цьому основна частина сучасного ринку праці визначається потребами у фахівцях з технічного захисту інформації у кіберпросторі.

Слід зазначити, що в даний час в Україні йде політика імплементації міжнародних стандартів ISO / AEC 27x серії, яка є моделлю для розробки, впровадження, моніторингу аналізу і підтримки та вдосконалення системи управління інформаційною безпекою, підґрунтям теоретико-методологічних основ якісної підготовки компетентних майбутніх фахівців з кібербезпеки.

Специфіка завдань, які розв'язують фахівці з кібербезпеки вимагають від них специфічних фахових компетенцій для забезпечення потреби в виявлені ознак ризиків кібербезпеки, в постійному моніторингу інформаційних потоків та систем зазначених об'єктів, протидії зовнішніх кібернетичних впливів. Зазначені фахівці являють собою частину інформаційної безпеки об'єкта критичної інфраструктури.

В процесі перепідготовки та фахової орієнтації для задоволенні потреб, що виникають в процесі професійної діяльності, а саме реагування на масштабні кіберзагрози і кібератаки необхідно використання широкого міждисциплінарного підходу для формування тематики навчального спецкурсу, який реалізує формування фахової компетенції майбутніх фахівців з кібербезпеки.

Формуватися професійної готовності фахівців до реалізації фахових компетенцій з кібербезпеки, які є базовими за специфікою діяльності здійснюється в процесі проходження подібних курсів. Зміст навчальних спецкурсів для формування професійної готовності до реалізації базових фахових компетенцій з кібербезпеки включає тематики теоретичних основ, визначення термінологічного апарату, управління ризиками, правові аспекти захисту інформації, організаційно-технічну складову, вивчення передового досвіду із реалізації сучасних досягнень менеджменту системи управління інформаційною безпекою, тематики щодо основних методів, підхо-

дів до реалізації захисту інформації, технологій кібербезпеки, що можуть використовуються при побудові та експлуатації сучасних інформаційних систем та СУІБ на об'єктах критичної інфраструктури та ін.

Відповідно до специфіки професійної діяльності фахівців з кібербезпеки необхідно включати тематики, практично спрямовані в залежності від способів реалізації ІСТ, ІТС, СУІБ та вимог чинного законодавства на основі моделі об'єкта критичної інфраструктури (полігону), а саме: на основі віртуалізації подібних інформаційних систем та мереж включатиме моделювання систем управління мережевою безпекою, здійснення моніторингу технологічних процесів мережі, операцій ОС, ІСТ та ІТС, адміністрування операційних систем, виявлення, управління та реагування на комп'ютерні інциденти, комп'ютерної криміналістики та техніки пошуку і фіксації цифрових доказів, проведення аудиту інформаційної та кібернетичної безпеки, включаючи тестування на вразливості всіх елементів мережевого обладнання та інших елементів СУІБ, рекомендації щодо забезпечення безперервності процесів та аварійного відновлення інформаційних активів, модернізації, вдосконалення СУІБ. Процес підвищення рівня фахової компетентності повинен бути безперервним в умовах розвиту й постійної модернізації інформаційних систем та організації їх захисту. Тим самим, на нашу думку, впровадження подібного підходу значно поліпшить якість фахової підготовки, реалізації у процесі професійної діяльності набутих фахових компетенцій фахівцями, що пройшли підвищення кваліфікації.

Література

1. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: аналітична доповідь. К.: НІСД, 2012. 102 с.

2. Бочков А. Категорирование критически важных объектов по уязвимости к возможным противоправным действиям. Экспертный подход. БДИ, №1 (82), январь-февраль 2009. С. 22–24.

3. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL : https://zakon.rada.gov.ua/ laws/show/2163-19 (Дата звернення: 8.03.2019)

4. Постанова КМУ від 23 серпня 2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави». URL : https://zakon.rada. gov.ua / laws/show/563-2016-%D0%BF (Дата звернення: 8.03.2019)

5. Рогов П. Д., Ворович Б. О., Ворона Т. О. Війна в кіберпросторі. К.: Оборонний вісник №1, 2017. Київ, 2017. С. 16–21.

УДК 343.451
Гавловський В.Д.
кандидат юридичних наук,
старший науковий співробітник,
Міжвідомчий науково-дослідний центр з проблем боротьби
з організованою злочинністю при РНБО України

ДО ПИТАННЯ ПОСИЛЕННЯ ЕФЕКТИВНОСТІ ПРОТИДІЇ КІБЕРАТАКАМ

Переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [1].

Низка потужних та складних кібератак на комп'ютерні мережі енергетичного, банківського, транспортного секторів, галузі зв'язку, які відбулися з початку 2014 року, стали невід'ємним компонентом гібридної війни, що її розв'язала Росія, і вкотре засвідчили, що і надалі агресором використовуватимуться кібератаки як інструмент геополітичного впливу.

Питанню забезпечення кібербезпеки перебувають у постійному полі зору РНБО України. З цієї проблематики була прийнято низку рішень, що були введені у дію Указами Президента України. Разом з тим існують певні проблемні питання щодо імплементації цих рішень.

Основну роль у протидії кібератакам відіграють підрозділи Служби безпеки України, зокрема Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ. Як відмітив керівник цього Департаменту О. Климчук, наразі в Службі безпеки України створена команда професіоналів, які забезпечують кібернетичну та інформаційну безпеку України, але для більш ефективної протидії кібератакам необхідно, серед іншого, отримання нових законодавчо-визначених інструментів протидії кібернетичним та інформаційними впливам [2].

На ефективність протидії кібератакам через несанкціоноване втручання в роботу державних інформаційних ресурсів, об'єктів критичної інфраструктури впливає відсутність кримінально-процесуальних важелів впливу Служби безпеки України на сферу таких злочинів, які наносять значну шкоду державній безпеці України. Одним з таких важелів є розмежування підслідності.

Про те, що на Службу безпеки України мають бути покладені в установленому порядку завдання розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури вказувалося ще в Стратегії кібербезпеки України [1].

Існує також потреба у розмежуванні кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені стосовно державних та інших інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури та інших об'єктів.

У липні 2017 року Рада національної безпеки і оборони України, розглянувши комплекс проблем у сфері забезпечення кібербезпеки, пов'язаних із наслідками здійснених масованих кібератак на державні електронні інформаційні ресурси та об'єкти критичної інфраструктури, доручила, зокрема: Кабінету Міністрів України у шестимісячний строк підготувати за участю Служби безпеки України та подати в установленому порядку на розгляд Верховної Ради України законопроект щодо розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідного розмежування підслідності.

Наприкінці березня 2018 року, на виконання цього пункту рішення РНБО України Адміністрацією Держспецзв'язку спільно зі Службою безпеки України підготовлено проект Закону України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо розмежування підслідності злочинів, вчинених у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури», який надійшов до Верховної Ради України 18 квітня 2018 року.

7 листопада 2018 року Комітет Верховної Ради України з питань законодавчого забезпечення правоохоронної діяльності рекомендував Верховній Раді України прийняти в першому читанні за основу цей законопроект (реєстр. № 8304).

При цьому Головне науково-експертне управління Апарату Верховної Ради України вважає, що за результатами розгляду в першому читанні законопроект доцільно повернути на доопрацювання з урахуванням висловлених зауважень та пропозицій. Отже, не варто сподіватися на прийняття цього Закону найближчим часом.

Варто вказати, що на сьогодні не виконано ще низку рішень Ради національної безпеки і оборони України, зокрема відсутній перелік об'єктів критичної інформаційної інфраструктури, на законодавчому рівні не визначено процедуру блокування Інтернет-сайтів, які містять протиправний контент, не створено єдиної інтерактивної бази даних про кіберінциденти тощо.

Література

1. Указ Президента України від 5.05.2016 року № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення 5.05.2019).

2. Інформаційна та кібербезпека в сучасному світі: досвід СБУ. URL: https://ua-news.liga.net/politics/opinion/informatsiyna-ta-kiberbezpeka-v-suchasnomu-sviti-dosvid-sbu (дата звернення 4.05.2019).

УДК 004.7(075)

Гордієнко С.Б.
кандидат технічних наук, доцент,
Національна академія СБ України
Козюра В.Д.
кандидат технічних наук, доцент,
Національна академія СБ України

АДРЕСАЦІЯ В МЕРЕЖАХ НОВОГО ПОКОЛІННЯ. ВИЗНАЧЕННЯ ПОНЯТТЯ, ЗАГАЛЬНІ ПРИНЦИПИ РЕАЛІЗАЦІЇ

На сьогоднішній день кожна людина, що користується смартфоном чи комп’ютером, так чи інакше використовує технології мультисервісних мереж зв’язку нового покоління (NGN, next generation networks) для передачі мови, тексту, відео та інших мультимедійних повідомлень. При цьому використовується в основному апаратура та програмне забезпечення мережі Інтернет. Це означає, що передача даних використовує не комутацію каналів як в традиційній телефонії, а комутацію пакетів, що підводить нас до думки, що для розподілення пакетів з різним вмістом мають застосовуватися особливі методи адресації [1-2].

Метою даної роботи є виявлення адресації в NGN та адресації в цілому; принципів роботи адресації, програмної та апаратної складової, що забезпечує реалізацію адресації, та інших нюансів пов’язаних з нею.

Актуальність обумовлена тим, що:

- нині багато компаній, що надають послуги зв’язку, використовують мережі нового покоління для отримання високонадійних і багатоцільових мереж, а адресація – це, по суті, засіб, який зв’язує всі вузли такої мережі [2];
- в мережі Інтернет відсутній структурований опис принципів адресації в мережах нового покоління [3-5];
- на даний момент активно впроваджуються нові методи адресації, які є більш адаптованими до використання в мережах нового покоління [6].

Для передачі даних в локальних і глобальних мережах пристрій-відправник має знати адресу пристрою-одержувача. Тому кожен мережевий комп'ютер (хост) має унікальну адресу, і не одну, а цілих три:

- фізичну або апаратну (MAC-адреса);
- мережеву (IP-адреса);
- символьну (звичайне ім'я комп'ютера або повне доменне ім'я).

Фізична (апаратна) адреса комп'ютера залежить від технології, за допомогою якої побудована мережа. У мережах Ethernet це MAC-адреса мережевого адаптера. MAC-адреса жорстко зашивається в мережеву карту її виробником і зазвичай записується у вигляді 12 шістнадцяткових цифр (наприклад, 00-03-BC-12-5D-4E). Це гарантовано унікальна адреса: перші шість символів ідентифікують фірму-виробника, яка стежить, щоб решта шість символів не повторювалися на виробничому конвеєрі. MAC-адресу вибирає виробник мережевого устаткування з виділеного для нього за ліцензією адресного простору. Коли у машини замінюється мережевий адаптер, то змінюється і її MAC-адреса.

Мережева адреса (IP-адреса) використовується в мережах стеку протоколів TCP/IP при обміні даними на мережному рівні, має довжину 32 біти і складається з чотирьох октет, кожний з яких може приймати значення від 0 до 255. IP-адреса комп'ютера (наприклад, 192.168.1.10), включає дві частини – номер мережі (ідентифікатор мережі) – це перші три октета (192.168.1) і номер мережевого комп'ютера (ідентифікатор хоста) – це четвертий октет (10).

IP-адреси комп'ютерів в різних мережах можуть мати однакові номери, а в межах однієї мережі не повинні повторюватися.

Щоб відокремити номер мережі та номер комп'ютера, застосовується маска мережі, яка являє собою такий же набір з чотирьох октетів, розділених крапками. Але, як правило, більшість цифр в ній – це 255 і 0.255, що вказує на біти, призначені для адреси мережі, в інших місцях (яким відповідає значення 0) повинна розташовуватися адреса комп'ютера. Чим менше значення маски, тим більше комп'ютерів об'єднано в дану підмережу. Маска мережі присвоюється комп'ютеру одночасно з IP-адресою.

Наприклад, мережа 192.168.0.0 з маскою 255.255.255.0 може містити в собі комп'ютери з адресами від 192.168.0.1 до 192.168.0.254. А мережа 192.168.0.0 з маскою 255.255.255.128 допускає адреси від 192.168.0.1 до 192.168.0.127.

Мережі з великою кількістю комп'ютерів зазвичай ділять на частини – підмережі. Такий поділ застосовується для забезпечення підвищеної безпеки і розмежування доступу до ресурсів різних підмереж. Комп'ютери різних підмереж не зможуть передавати пакети один одному без спеціального пристрою – маршрутизатора, а, отже, ніхто не зможе проникнути в захищену таким чином підмережу. Для створення підмереж треба частину місця в IP-адресі, відведеної для хоста, віддать під номери підмереж.

Наприклад, в локальній мережі є 30 комп'ютерів і потрібно налаштувати їх так, щоб 20 комп'ютерів могли спілкуватися між собою, але не змогли передавати і приймати дані від решти 10 комп'ютерів, які також повинні спілкуватися тільки між собою. У такій ситуації локальна мережа поділяється на дві підмережі: перша підмережа має комп'ютери з адресами 192.168.1.1 – 192.168.1.20, а в друга – з адресами 192.168.2.1 – 192.168.2.10.

Крім фізичної і мережевої адрес комп'ютер може також мати символьну адресу – ім'я комп'ютера. Ім'я комп'ютера – це більш зручне і зрозуміле для людини позначення комп'ютера в мережі. Розрізняють NetBIOS імена і повні доменні імена комп'ютерів.

Імена NetBIOS використовуються в однорангових локальних мережах, в яких комп'ютери організовані в робочі групи. NetBIOS – це протокол для взаємодії програм через комп'ютерну мережу, який розпізнає звичайні літерні імена комп'ютерів і відповідає за передачу даних між ними. Провідник Windows для перегляду локальної мережі надає папку Мережеве оточення, автоматично відображає імена NetBIOS-комп'ютерів у локальній мережі. Ім'я NetBIOS може містити не більше 15 символів та має бути англійською мовою.

Висновки: станом на сьогодні спостерігається тенденція щодо глобалізації різних телекомунікаційних мереж та їх об'єднання в більші системи, що мають надавати широкий спектр послуг. В таких мережах важливу функцію виконує адресація повідомлень. Повідомлення (текст, аудіо, відео та ін.) пакуються в пакети, які в свою чергу можуть доставлятися до одержувача через різні канали зв'язку, як прямим (найкоротшим) так і обхідним шляхом (комутація пакетів). Це означає, що є ряд проблем в реалізації обміну мультимедіа за допомогою комутації пакетів таких як:

- у випадку передачі аудіо чи відео повідомлень в режимі реального часу потрібно реалізувати аналого-цифрове перетворення сигналу з подальшим його кодуванням та передачею (за це, як правило, відповідає технологія VoIP);
- необхідно в режимі реального часу коректне оформляти пакети до передачі, для того щоб інформація не втрачалася при передачі (за це відповідає протокол RTP).

Література

1. NGN. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/NGN.

2. Современные тенденции развития телекоммуникационных сетей. [Електронний ресурс]. – Режим доступу: http://sernam.ru/book_history.php?id=25.

3. Класифікація IP-адрес. [Електронний ресурс]. – Режим доступу: https://studopedia.su/17_17340_klasifikatsiya-IP-adres.html. -

4. Порядок розподілу IP-адрес. [Електронний ресурс]. – Режим доступу: http://www.matveev.kiev.ua/archnet/gl5/012.htm.

5. Принципи трансляції мережевих адрес. [Електронний ресурс]. – Режим доступу: http://um.co.ua/9/9-16/9-169782.html.

6. Основы компьютерных сетей. IP-адресация. [Електронний ресурс]. – Режим доступу: http://net.e-publish.ru/p234aa1.html.

УДК 343.9.024 : 004.056

Гуцалюк М.В.
кандидат юридичних наук,
старший науковий співробітник, доцент,
Міжвідомчийнауково-дослідний центр
з проблем боротьби з організованою злочинністю
при РНБО України

ОКРЕМІ АСПЕКТИ БОРОТЬБИ З ОРГАНІЗОВАНОЮ КІБЕРЗЛОЧИННІСТЮ

У сучасному інформаційному суспільстві з розвитком інформаційних технологій продовжує розвиватися і кіберзлочинність, яка приймає нові форми та орієнтується на нові напрями. Генеральний секретар Організації Об'єднаних Націй Антоніу Гутерріш на 27-й сесії Комісії ООН з попередження злочинності та кримінального правосуддя зазначив, що нові технології надають людству значних переваг, але, разом з тим, створюють нові форми злочинності. Збитки світової економіки від кіберзлочинності оцінюються у $ 1,5 трлн на рік. А за негативним сценарієм у 2019 році вони сягатимуть $ 2 трлн [1].

Практично всі фахівці визнають, що ситуація з кіберзлочинністю у світі має тенденцію до погіршення. Значних збитків зокрема завдаютьбезпрецедентного масштабу кібератаки, які сталися минулими роками та продовжуютьохоплювати багато країн світу.

Однією з небезпечних тенденцій кіберзлочинності слід визначити посилення її організованості. Серед причин посилення організованості злочинної діяльності в мережі Інтернет можна вважати те, що така діяльність стає більш вигідною, ніж інші способи незаконного збагачення. При цьому Інтернет використовується як основний засіб вчинення традиційних злочинів – шахрайства, крадіжок, вимагання, продажу наркотичних засобів тощо.

Небезпечною тенденцією є також формування бізнес-моделі «Злочин як послуга». У мережі сформувався та продовжує розширюватися ринок хакерських послуг, які можливо придбати за відносно невеликі кошти. Наприклад, 5-хвилинна атака на Інтернет-магазин може коштувати всього

лише 5 доларів США, тоді як конкретному бізнесу вона коштуватиме значно більше.

Замість того, щоб вивчити технологію проведення складних кібератак, наприклад, APT-атак (advanced persistent threat – APT), кіберзлочинці спеціалізуються набільшдоступніших технологіях. Коли їм потрібно здійснити, наприклад, несанкціонований доступ до бази даних,що виходить за межі їхньої компетенції, їм потрібно лише знайти когось, хто запропонує відповідний інструмент або послугу в мережі Даркнет. Також на основі конкретних навичок кіберзлочинці можуть об'єднуватися у більш координовані групи для вчинення більш складних злочинів. Такі об'єднання часто є тимчасовими і створюються лише для втілення конкретного злочинного задуму, а потім розпадаються. Це ускладнює їх ідентифікацію правоохоронцями порівняно з традиційними організованими злочинними групами. Зважаючи на транснаціональний характер кіберзлочинів, такий ринок поширюється на багато країн, у тому числі й Україну. Наприклад, під час проведення операції Op CORPASS британські правоохоронці виявили, що шкідливе програмне забезпечення протиправної діяльності в багатьох країнах світу виготовлялося в Україні [2].

Уже традиційно метою злочинних організацій є кошти банківських установ. У березні 2018 року в місті Аліканте в Іспанії заарештували лідера організованого злочинного угруповання (ОЗУ) 34-річного українця К. Дане ОЗУ розпочало свою діяльність у 2013 році, здійснюючи кібератаки на банки, системи електронних платежів та фінансові установи, використовуючи свої власні розробки, відомі як Carbanak і Cobalt.

За даними слідства, потерпілими від злочинної діяльності ОЗУ стали понад 100 банків із 40 країн світу. За попередніми даними, сума викраденого перевищує 1 мільярд євро, хоча мова може йти і про значно більшу суму (до 10 мільярдів). Пізніше у США заарештували ще трьох громадян України – членів ОЗУ Carbanak або ж Fin7 [3].

Незважаючи на значну кількість виявлених кіберзлочинів в Україні та збільшення кількості осіб, засуджених за статтями, передбаченими Розділом XVI КК України (ст. 361 – 361-3), за даними судової статистики – 70 у 2018 році проти 42 у 2017 році (+ 66 %), протягом цих років лише по 2 особи були позбавлені волі на строк до 5 років. Тобто часто покарання за вчинення кіберзлочинів обмежується лише невеликим штрафом – тому, що ці злочини кваліфікуються як злочини середньої тяжкості.

Наприклад, громадянину з Миколаєва за поширення в Інтернет шкідливого програмного забезпечення для віддаленого доступу до комп'ютерів у грудні 2017 року було призначено штраф у розмірі 11900 грн [4], а студент зі Львова за поширення вірусу-вимагача у 2018 році взагалі був звільнений від кримінальної відповідальності та лише оплатив проведення судових експертиз [5].

На нашу думку, невелика кількість засуджених за вчинення кіберзлочинів пояснюється також неврегульованістю на законодавчому рівні (КПК України) використання електронних доказів у кримінальному процесі.

Зазначимо також, що з 1 січня 2019 року державним стандартом ДСТУ 27037 було введено в дію Настанову для ідентифікації, збирання та збереження цифрових доказів, які слід застосовувати для розслідування не тільки кіберзлочинів, але й традиційних злочинів. Проте цей документ розповсюджується згідно з ч. 4 статті 24 Закону України «Про стандартизацію» лише на договірній (платній) основі, а його вартість досить висока, що перешкоджає використанню даної Настанови практичними підрозділами правоохоронних органів.

Література

1. Киберпреступники наживаются на самых бедных URL: https://www.unodc.org/unodc/ru/frontpage/2018/May/much-work-to-do-and-no-time-to-waste-in-cybercrime-fight--says-un-chief.html (дата звернення: 19.02.2019).
2. Правоохранители Украины и Великобритании ищут украинского хакера URL:http://internetua.com/pravoohraniteli-ukrainy-i-velikobritanii-isxut-ukrainskogo-hakera(дата звернення 04.02.2019).
3. У США арештували українських хакерів URL: https://www.pravda.com.ua/news/2018/08/1/7188031/ (дата звернення 27.12.2018).
4. Хакер-неудачник заплатит 14 тысяч за распространение компьютерного вируса URL: http://internetua.com/haker-neudacsnik-zaplatit-14-tysyacs-za-rasprostranenie-kompuaternogo-virusa(дата звернення 04.02.2019).
5. Пойманный хакер заплатит 47 тысяч за судебные экспертизы URL: http://internetua.com/poymannyi-haker-zaplatit-47-tysyacs-za-sudebnye-ekspertizy(дата звернення 04.02.2019).

УДК 004.056.523:57.087.1(043.2)

Давиденко А.М.
кандидат технічних наук,
старший науковий співробітник
Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
Висоцька О.О.
Національний авіаційний університет

МОНІТОРИНГ ФУНКЦІОНАЛЬНОГО СТАНУ ПРЕДСТАВНИКІВ КРИТИЧНИХ ПРОФЕСІЙ, ЗА ДОПОМОГОЮ АНАЛІЗУ ЇХ КЛАВІАТУРНОГО ПОЧЕРКУ

Безпека держави невід’ємно залежить від безпеки життя її громадян. Існує ряд професій, від уважності та зосередженості представників кот-

рих, напряму залежить життя багатьох людей. Серед них, наприклад, авіадиспетчера та військові логісти. Тобто, у випадку, якщо внаслідок помилки, авіадиспетчер неправильно скоординує рух літаків, чи військовий логістик спрямує машину або не з тим військовим спорядженням, що потрібно, або не в той пункт призначення, можливі значні людські жертви. Подібні помилки трапляються переважно через неуважність і низький рівень зосередженості даних співробітників. Для мінімізації цих помилок, необхідно під час роботи, контролювати людські характеристики, які демонструють рівень уважності і зосередженості працівника. Тобто створення системи контролю та моніторингу роботи працівників, чия уважність є принциповою, є актуальною задачею безпеки держави.

Для вищезазначеного контрою та моніторингу є сенс аналізувати динамічні біометричні характеристики людини [1]. А враховуючи той факт, що у всіх зазначених сферах діяльності, під час роботи, постійно використовуються комп'ютери, доцільно аналізувати саме клавіатурний почерк людини. Якщо під час роботи за комп'ютером, користувач відволікається, тоді динаміка його роботи на клавіатурі відхиляється відносно нормальної, для нього, динаміки роботи, а якщо людина неуважна, тоді кількість зроблених помилок буде значно більша, ніж у інших користувачів. В даній роботі в якості параметрів, що аналізуються, використовуються часові інтервали між натисканням двох сусідніх символів слова (фрази) [1]. Для досягнення більшої імовірності правильного розпізнавання, можна додатково ще аналізувати часові інтервали між натисканням та відпусканням кожної клавіші. При цьому задачу моніторингу роботи користувачів комп'ютерної системи, можна звести до задачі класифікації або розпізнавання образів. Для реалізації даного методу розпізнавання образів був обраний один з найбільш ефективних механізмів рішення даної задачі – нейронні мережі.

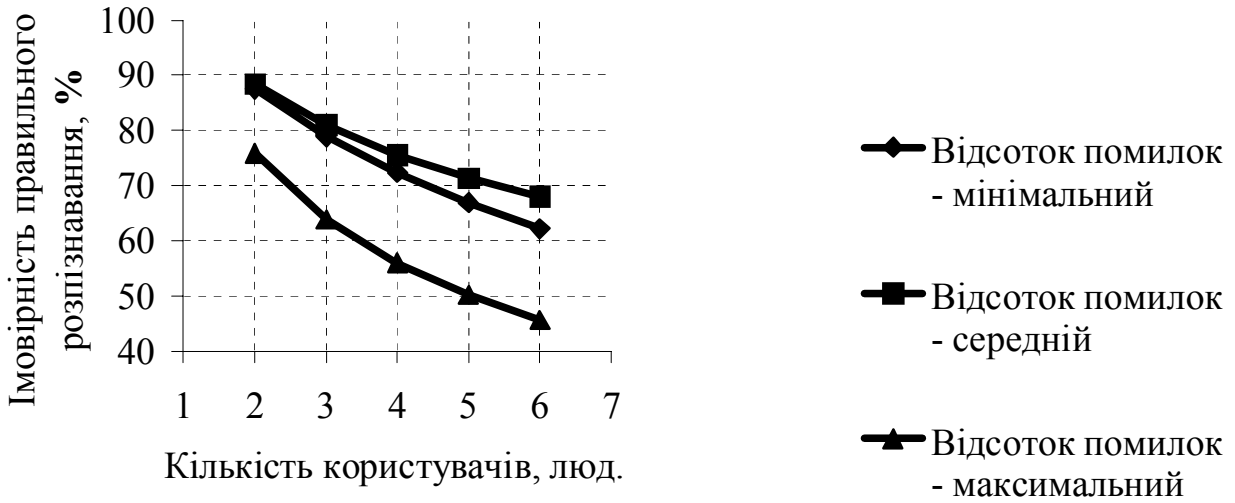
Робота розробленої системи моніторингу, як і будь-якої біометричної системи розпізнавання, складається з двох етапів: накопичення бази даних навчальних зразків клавіатурного почерку всіх користувачів системи; розпізнавання об'єктів, на основі накопичених раніше зразків.

В даному випадку є сенс накопичення зразків почерку продовжувати і під час етапу розпізнавання. Розмір необхідної бази даних навчальних зразків залежить від біометричного метода, що використовується. Враховуючи, що дана система аналізує динамічний параметр людини, який не є стовідсотково стабільним, для розпізнавання, в базі даних необхідна наявність хоча б декількох сотень навчальних зразків почерку для кожного співробітника. Від кількості накопичених зразків почерку для кожного користувача, залежить імовірність правильної роботи системи моніторингу.

Значний вплив на якість розпізнавання має кількість параметрів, що аналізуються. Експерименти, що були проведені, показали значне зростання імовірності правильного розпізнавання, при збільшенні кількості параметрів з 3 до 6 і незначний зріст, при збільшенні кількості з 6 до 11.

Якість розпізнавання почерку людини та моніторингу його відхилень залежить від якості обраних для аналізу параметрів. Необхідно аналізувати час набору символів тих слів, які характерні для сфери діяльності саме цієї організації.

Уважність і зміну уважності працівника можна контролювати не тільки за динамікою його роботи на клавіатурі, а й за кількістю і типовістю помилок, що він робить [1]. Тобто необхідно фіксувати не тільки часові інтервали між натисканням відповідних клавіш, а й кількість зроблених помилок (введення неправильних символів), після чого обраховувати відсоток помилок, які робить користувач системи. Крім того, на якість роботи даної системи моніторингу, має значний вплив амплітуда відсотка помилок у користувачів (рис. 1).



Всі ці фактори необхідно враховувати під час розробки та налаштування системи контролю та моніторингу.

На основі всього вищесказаного, можна зробити висновок, що використання розробленої системи контролю та моніторингу роботи працівників, чия уважність є принциповою, є ефективним способом вирішення поставленої задачі.

Література

1. Висоцька О.О. Моніторинг роботи користувачів комп'ютерних систем за допомогою технологій розпізнавання за клавіатурним почерком / О.О. Висоцька// Моделювання та інформаційні технології. Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН Україні. – К.:ІПМЕ, 2018. – Вип. 84. – С. 119-125.

УДК 044.056
Даник Ю.Г.
доктор технічних наук, професор
Войтко О.В.
кандидат військових наук,
Національний університет оборони України

ДЕЯКІ ОСОБЛИВОСТІ СТВОРЕННЯ КІБЕРПОЛІГОНІВ ДЛЯ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

Реалії сьогодення доводять, що сучасні методи та способи реалізації гібридних впливів супроводжуються значним потоком динамічно змінюваних кризових ситуацій. Їм властива апріорна невизначеність за метою, суб'єктом та об'єктом впливу, змістом, сутністю і способами реалізації. Технологічно побудова відомих систем протидії таким кризовим ситуаціям, форми і способи їх застосування орієнтовані на формування статичної надмірної структури системи. Розподіл завдань між усіма складовими системи здійснюється рівномірно з вибірковістю елементів лише за їх призначенням. Збільшення кількості та щільності потоку кризових ситуацій, кіберінцидентів та їх типів відпрацьовується збільшенням елементів структури. Це породжує інформаційну надмірність даних та ускладнення їх передачі і обробки. На таких самих принципах побудовані програмні засоби реалізації процесів оперативного виявлення, захисту та активної протидії інформаційним загрозам в кіберпросторі. Такі підходи не є дієвими в реальних умовах обстановки, під час застосування противником переважаючих або рівних за складом та рівнем розвитку засобів інформаційного впливу і здійснення масованих інформаційних та кібератак, які супроводжуються іншими несиловими і силовими методами досягнення мети конфлікту.

Таким чином, має місце актуальна проблема створення кіберполігонів для дослідження комплексних кібердій та підготовки фахівців з кібербезпеки з метою виконання завдань щодо розробки методологічного забезпечення автоматизованого моніторингу, аналітичної обробки інформації, прогнозування, планування та здійснення заходів пасивної і активної протидій інформаційним загрозам в кіберпросторі. Її вирішення та підвищення ефективності комплексу заходів забезпечення інформаційної та кібербезпеки в кіберпросторі з відпрацюванням заходів протидії гібридним впливам в цілому вимагає наявності методологічних основ створення та організації ефективного застосування відповідних кіберполігонов [1].

Розробка та створення кіберполігону для дослідження і багатостороннього відпрацювання заходів протидії гібридним впливам в кіберпросторі реалізується загальнонауковими методами теорії системного аналізу. Ме-

тодика створення кіберполігону для відпрацювання інноваційних засобів і заходів забезпечення інформаційної та кібербезпеки в кіберпросторі в умовах гібридних конфліктів різної інтенсивності і змісту, з відпрацюванням заходів протидії гібридним впливам базується на здійсненні комплексу наукових досліджень фундаментального і прикладного характеру, реалізації інженерних завдань і організаційно-технічних заходів.

Розробка та виготовлення діючих кіберполігонів здійснюється з базових дискретних компонентів. До складу кіберполігону повинні входити два і більше ідентичних за призначенням, складом, функціональними можливостями комплектів спеціалізованих програмно-апаратних комплексів:

комплект засобів, які імітують дії сил і засобів, що здійснюють кібервпливи та виконують завдання кібероборони;

комплект засобів які здійснюють тестування.

Комплект засобів які імітують дії сил і засобів, що здійснюють кібервпливи та виконують завдання кібероборони, призначений для дослідження кібердій, забезпечення кібербезпеки сервісів та служб дата-центру кіберполігону, а також оцінки впливів на особовий склад через кіберпростір.

Комплект засобів які забезпечують тестування призначений для оцінки функціональної стійкості сервісів та служб дата-центру кіберполігону.

Комплекс тестування являє собою потужний дата-центр, сервіси та служби якого, з одного боку, захищаються силами та засобами що імітують сили кібероборони, з іншої – тестуються на кіберзахищеність силами та засобами другого комплекту.

Наявність таких кіберполігонів надасть можливість проведення з їх використанням кібернавчань та командно-штабних навчань і тренувань з елементами відпрацювання дій в умовах комплексних деструктивних інформаційних та кібервпливів, а також оцінювати прийняте рішення командиром підрозділу з кібербезпеки.

Процес прийняття рішення особовим складом підрозділу, який проходить тренінги з кібербезпеки доцільно здійснювати за типовими процедурами та стандартами прийнятими в країнах – членах НАТО [2].

Пропонується наступний порядок дій щодо прийняття рішення особовим складом, який проходить підготовку:

1 етап: Отримання завдання.

2 етап: Аналіз завдання має включати: аналіз та усвідомлення директивних документів; здійснення попереднього оцінювання; визначення першочергових завдань; оцінку наявних сил та засобів; визначення обмежень на проведення дій (сканування портів, проведення DDoS-атак, прослуховування та перехоплення потоку інформації в каналах мережі, псевдо санкціоноване проникнення в підсистему захисту, знищення, спотворення, крадіжка інформації, блокування доступу до неї в підсистемі кібероборони за допомогою засобів спеціального програмного впливу тощо); ви-

значення критичних фактів, визначення ризиків підрозділу в ході проведення дій; визначення критично-необхідної розвідувальної інформації; розроблення попередньої матриці синхронізації ведення розвідки, спостереження та збору розвідувальної інформації; розроблення плану ведення розвідки спостереження та збору розвідувальної інформації; встановлення часових показників розроблення плану операції; розробку цілей та завдань дій, доповідь результатів аналізу операції, розробку критеріїв оцінювання варіантів способу дій, видання попереднього розпорядження.

3 етап: Розробка варіантів способу дій має включати: оцінювання можливостей підрозділу, розробку варіантів способу дій; розробка концепції ведення дій; визначення завдань підрозділу; вибір варіантів способів дій.

4 етап: Розіграш варіантів способу дій має включати: визначити склад та інструменти, необхідні для розіграшу; список відомих подій, які мають критичне значення на хід операцій; обрати метод проведення моделювання; провести моделювання та оцінити результати; провести брифінг по результатам моделювання.

5 етап: Порівняння варіантів способів дій має включати: проведення аналізу переваг та недоліків способу дій; порівняння варіантів способу дій; провести брифінг з обрання варіанту способу дій.

6 етап: Затвердження варіанту способу дій має включати: .

7 етап: Розробка наказу.

Література

1. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки: монографія; за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ, 2016. 636 с.

2. GTA 33-01-001 – Military Information Support Operations in the Military Decisionmaking Process. April, 2014.

УДК 342.9

Дмитренко Е.С.
доктор юридичних наук, професор,
ДВНЗ «Київський національний економічний університет
імені Вадима Гетьмана»

ОСОБЛИВОСТІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БАНКІВСЬКОЇ СИСТЕМИ У СУЧАСНИХ УМОВАХ

Розвиток інформаційних технологій у сфері банківської діяльності спричинює виникнення різних ризиків як для банків, так і для їхніх клієнтів під час здійснення банківських операцій. Функції щодо виявлення та зменшення негативного впливу таких ризиків та забезпечення безпеки

здійснення банківських операцій покладені відповідно до п. 7 ч. 1 ст. 7 Закону України «Про Національний банк України» від 20.05. 1999 р. № 679-XIV на Національний банк України (далі – НБУ). Так, НБУ визначає напрями розвитку сучасних електронних банківських технологій, створює та забезпечує безперервне, надійне та ефективне функціонування, розвиток створених ним платіжних та облікових систем, контролює створення платіжних інструментів, систем автоматизації банківської діяльності та засобів захисту банківської інформації. Окрім того, ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII НБУ віднесено до суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки.

З метою реалізації цих функцій постановою Правлінням НБУ «Про затвердження нормативно-правових актів з питань інформаційної безпеки» від 26.11.2015 р. № 829 було затверджено Положення про захист електронних банківських документів з використанням засобів захисту інформації НБУ. Зокрема, п. 9 цього Положення було визначено, що основною метою засобів захисту інформації НБУ, які використовуються в системі електронних платежів НБУ та інформаційних задачах (ЗЗІ), є забезпечення конфіденційності та цілісності інформації в електронній формі на будь-якому етапі її оброблення, а також сувора автентифікація учасників системи електронних платежів НБУ (СЕП), учасників інформаційних задач і фахівців організацій, які беруть участь у підготовці й обробленні електронних документів.

Окрім того, відповідно до п. 19 зазначеного Положення однією з умов для отримання ЗЗІ є приєднання організації-замовника до Єдиного договору для отримання таких видів послуг НБУ, як: розрахунково-інформаційне обслуговування в системі електронних платежів НБУ (для учасників СЕП); система електронної пошти НБУ (далі – система ЕП); із надання в користування засобів захисту інформації НБУ. Разом із тим для організацій-замовників, які є державними установами (Державна казначейська служба України, Державна служба фінансового моніторингу України, Державна фіскальна служба України, Національне антикорупційне бюро України, Державна установа «Офіс адміністрування проектів міжнародного фінансового співробітництва», Державна іпотечна установа, Фонд гарантування вкладів фізичних осіб, Центральна виборча комісія) такою умовою є укладення договору про використання засобів захисту інформації НБУ між організацією-замовником та НБУ та підключення до системи ЕП.

Поряд із цим іншими умовами для отримання ЗЗІ є: забезпечення відповідності приміщень, у яких будуть оброблятися електронні банківські документи, використовуються та зберігаються ЗЗІ, вимогам, визначеним Правилами; призначення посадових осіб, відповідальних за зберігання та використання ЗЗІ тощо.

Варто зазначити, що забезпечення інформаційної безпеки банку здійснюється, зокрема, за допомогою технологічних засобів контролю, вбудованих в програмно-технічні комплекси СЕП, а також шляхом внутрішнього контролю за функціонуванням системи безпеки розрахунків.

Окремо зауважимо, що у структурі НБУ є окремий структурний підрозділ – Департамент безпеки, однією з основних функцій якого є розроблення та реалізація стратегії і політики інформаційної безпеки НБУ, упровадження новітніх технологій у частині забезпечення ефективного і цілеспрямованого захисту інформації в інформаційній інфраструктурі НБУ та банківської системи України. Так, Департаментом безпеки НБУ відповідно до Положення про порядок перевірки стану інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України, затвердженого постановою Правління НБУ «Про затвердження нормативно-правових актів з питань інформаційної безпеки» від 26.11.2015 р. № 829, здійснюється зовнішній контроль за функціонуванням ЗЗІ за допомогою таких процедур, як проведення планових та позапланових перевірок стану інформаційної безпеки в організаціях.

Ще одним важливим нормативно-правовим актом, який було прийнято з метою забезпечення ефективного захисту від кібератак на банківські установи, є Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене постановою Правління НБУ від 28.09.2017 р.№ 95. Відповідно до цього Положення на банківську установу покладається обов’язок утворити власну систему управління інформаційною безпекою та створити підрозділ з інформаційної безпеки не менше як із двох працівників зі складу штатних працівників банку, а також призначити відповідальну особу за інформаційну безпеку банку, яка має забезпечувати стратегічне керівництво з питань інформаційної безпеки банку та контроль за впровадженням заходів безпеки інформації в банку.

З огляду на зазначене, можна зробити висновок про створення правових основ системи кіберзахисту банківської системи в Україні. Пріоритетними напрямами забезпечення кібербезпеки банківської системи України, на наш погляд, є: моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; забезпечення захищеності банків від кібератак; захист інформаційних ресурсів банку з урахуванням практики держав-членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки.

УДК 364
Дмитренко Ю.П.
кандидат юридичних наук, професор,
Національна академія Служби безпеки України

КОМПЛЕКТУВАННЯ ПІДРОЗДІЛІВ СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ: СОЦІАЛЬНО-ПРАВОВІ ПРОБЛЕМИ

В сучасних умовах інтеграції інформаційних процесів в різні сфери суспільного життя у багатьох державах виділяються значні кошти на створення та вдосконалення ефективних систем захисту критичної інфраструктури від загроз кібернетичного характеру.

У провідних країнах світу вже сформовані загальнодержавні системи кібернетичної безпеки – як найбільш оптимальні організаційно-функціональні структури, що здатні за короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам [1, с. 312]. В Україні також відбувається становлення системи забезпечення кібернетичної безпеки. Проте, практика показує недосконаліть національної системи кібербезпеки, виявляє суттєві недоліки в кадровому забезпеченні її суб'єктів. Приклади кібератак зі спробами втручання в електронну виборчу систему, зокрема під час проведення виборів у різних країнах (у т.ч. США, Франції та ін.) визначають надзвичайну актуальність цієї теми. До цього відповідні структури-суб'єкти забезпечення кібернетичної безпеки, повинні бути готовими в Україні особливо зараз, в період проведення президентських та парламентських виборів. В умовах ведення «гібридної війни» Російською Федерацією проти України необхідність у кваліфікованих кадрах у цій сфері постійно зростає. Від їх професіоналізму, компетентності, сумлінної праці, дисциплінованості та відповідальності залежить успіх діяльності у будь-якій сфері. Це стосується і питань забезпечення інформаційної та кібернетичної безпеки.

СБ України належить до суб'єктів забезпечення кібернетичної безпеки, де існує проблема якісного кадрового забезпечення. Метою кадрового забезпечення службової діяльності є своєчасне, ефективне комплектування підрозділів професіоналами, формування і збереження кадрового резерву, постійне підвищення професійного рівня співробітників, удосконалення механізму раціонального використання кадрового потенціалу СБ України, який відповідає покладеним на підрозділи органів і закладів завдань та забезпечує їх ефективне виконання.

На сьогодні все ще існує проблема якісного комплектування і підрозділів СБ України у зазначеній сфері співробітниками-фахівцями, спроможними якісно виконувати покладені чинним законодавством завдання з

ефективного забезпечення державної безпеки. Найбільшою проблемою залучення високопрофесійних фахівців до служби (роботи) в підрозділи суб'єктів забезпечення кібернетичної безпеки держави є недостатній рівень пропонованого матеріального, зокрема, грошового забезпечення за відповідними посадами. Як відомо співробітники ІТ сфери на сьогодні є одними з найбільш високооплачуваних фахівців у світі, тому питання їх мотивації при комплектуванні підрозділів сектору безпеки і оборони є досить актуальним. Значна кількість фахівців ІТ сфери нині взагалі з України виїжджає на роботу в інші держави.

Критерії відбору до кандидатів на службу (роботу) в СБ України є досить високими. Так, під час роботи з кандидатами на службу (роботу) в СБ України керівниками підрозділів та органів СБ України повинна акцентуватися увага на: якісному відборі співробітників, з врахуванням професійних та особистих якостей кандидатів на службу (роботу); доведення реальної інформації щодо питань фактичних соціальних гарантій кадрів та ін. Тому метою вирішення цього питання важливе значення має встановлення високих соціальних гарантій для співробітників.

У контексті інтеграції до правового простору ЄС, в Україні здійснюється реформування і сфери соціального захисту. Проте багато бажаючих кандидатів на службу (роботу) не відповідають на сьогодні за станом здоров'я, своїми професійними та особистими якостями визначеним вимогам.

Одним із напрямів вирішення зазначеної проблеми є підготовка кадрів для системи забезпечення кібернетичної безпеки, шляхом залучення високопрофесійного викладацького складу та жорсткого відбору кандидатів на навчання. Проте, одночасно повинні бути створені і високі соціальні гарантії для професіоналів, інакше досвідчені працівники, з часом, все одно будуть звільнятись. Отже, викладений вище аналіз ситуації, яка склалася на практиці з проблем комплектування підрозділів, установ системи забезпечення кібернетичної безпеки, дає підстави зробити *висновки:* з метою підвищення рівня якісного складу кандидатів на службу (роботу) системи забезпечення кібернетичної безпеки необхідно підвищити рівень соціальних гарантій (повинен бути не нищий ніж у співробітників зазначеної сфери); встановити доплати досвідченим співробітникам підрозділів (викладачам, наставникам), що відбирають кандидатів на службу (роботу), та навчають студентів, молодих співробітників (працівників); закріпити у нормативних актах обов'язкове відпрацювання (служби) випускників навчальних закладів (молодих спеціалістів) у підрозділах, які їх відбирали на навчання (не менше 3 роки). Запропоновані заходи сприятимуть стабілізації питання якісного комплектування відповідних підрозділів та підвищенню ефективності забезпечення безпеки у цій сфері.

Література

1. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 312-320.

2. Ліпкан В. А., Діордіца І. В. Національна система кібербезпеки як складова системи забезпечення національної безпеки України / В. А. Ліпкан, І. В. Діордіца [Електронний ресурс]. — Режим доступу : http://goal-int.org/natsionalna-sistema-kiberbezpeki-yak-skladovoyi-sistemi-zabezpechennya-natsionalnoyi-bezpeki-ukrayini/.

УДК 342.518(477)+342.571 (477)+351.86(477)

Доронін І.М.
кандидат юридичних наук, доцент,
НДІ інформатики і права НАПрН України

ОРГАНІЗАЦІЯ ЗВІТУВАННЯ СУБ'ЄКТІВ КІБЕРБЕЗПЕКИ

Звітування державних органів перед суспільством є важливою складовою забезпечення належного громадського контролю. У сучасному світі в умовах розвитку інформаційного суспільства трансформується і зміст звітування.

Чинне законодавство у сфері забезпечення кібербезпеки визначає порядок звітування перед суспільством суб'єктів кібербезпеки. Водночас, останні законодавчі новації не змінили усталених підходів щодо загальної організації звітування державних органів, а отже і не усунули існуючих проблем.

Загалом проблемне поле організації звітування у сфері національної безпеки і оборони полягає у наступному. Починаючи з 1990-х років законодавчо встановлено звітування державних органів у сфері безпеки і оборони перед Верховною Радою України. Але законодавча регламентація звітування досить різна. Так, наприклад, Закон України «Про Службу безпеки України» визначає щорічне подання звіту про діяльність Служби безпеки України (СБУ). Але стаття 31 зазначеного Закону і у першій редакції, і з урахуванням змін, внесених Законом України від 07.10.2010 № 2592-VI, не визначає форму такого звіту і порядок його подання. Більш того, термін «щорічний» не встановлює чіткої дати (або періоду) його подання. Видається, що наведене вище заширoке законодавче формулювання змісту такого звіту не сприяє належному правовому регулюванню підзвітності. При цьому не слід забувати і про практику діяльності державних органів у галузі зв'язків з громадськістю, яка склалась. Наприклад, на початку 2017 року було повідомлено про видання «друкованого публічного звіту» Служби безпеки України «за європейськими принципами», який щорічним не став, а його структура, зміст, форма подання інформації та

наповнення визначається самим державним органом. Окрім цього у практиці звітування СБУ за останні 15 років здійснювалось видання «білих книг», ювілейних видань, проблемних звітів, періодичних бюлетенів з окремих питань тощо. Щодо діяльності Управління державної охорони (УДО) законодавчо визначено наступний порядок. Стаття 25 Закону України «Про державну охорону органів державної влади України та посадових осіб» досить чітко встановлює порядок звітування, визначаючи, що начальник Управління щорічно, до 1 лютого наступного за звітнім року, подає Верховній Раді України письмовий звіт про діяльність Управління. Водночас, відсутні будь-які законодавчі вимоги щодо змісту та обсягу такого звіту, що дозволяє виконати законодавчий припис суто формально. На відміну від цього, процедура звітування перед Верховною Радою інших суб'єктів забезпечення безпеки і оборони (СЗР, інші розвідувальні органи; Збройні Сили тощо) законодавчо не врегульована.

Прийнятий нещодавно Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII також передбачає процедуру звітування у межах контролю за законністю заходів із забезпечення кібербезпеки. Зокрема, ст. 15 Закону передбачено, що «основні суб'єкти», визначені ч. 3 ст. 8 цього ж Закону, «подають один раз на рік звіти про стан виконання ними заходів з питань забезпечення кібербезпеки держави, віднесених до їх компетенції, які мають містити, зокрема, інформацію про результати проведення незалежного аудиту їхньої діяльності». При цьому адресат звітів законодавчо визначено недосконало, оскільки з тексту Закону вбачається, що такий звіт подається не до Верховної Ради України, а до її Комітету. До числа зазначених суб'єктів належать Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. Деякі із цих суб'єктів мають звітувати у загальному порядку, визначеному спеціальними законодавчими актами. Інші ж мають подавати окремий звіт. Законодавець визначив фактично єдину вимогу до такого звіту – наявність інформації про результати проведення незалежного аудиту. Формулювання щодо «наявності інформації» можливо варто було б замінити іншим терміном, що визначав би висновки такого аудиту, або визначити необхідність безпосереднього подання самого висновку аудиту як частини звіту.

Окрім цього, розуміння поняття «незалежного аудиту» в сфері кібербезпеки на рівні фахівців не викликає питань, оскільки існують відповідні міжнародні стандарти, органи сертифікації та сертифіковані процедури, а також організації, що їх здійснюють. Практика застосування законодавства скоріше за все буде здійснюватись саме таким шляхом. Але законодавець визначив у тексті Закону досить багато споріднених термінів, що

можливо мають різне значення. Зокрема, у тексті Закону згадуються «аудит інформаційної безпеки», «аудит захищеності», «аудит стану кіберзахисту», «аудит діяльності» і «аудит діяльності щодо ефективності». Множинність термінів не сприятиме чіткості правозастосування.

Підсумовуючи викладене можливо прийти до загального висновку про необхідність встановлення законодавчо вимог до порядку звітування суб'єктів кібербезпеки так само як у цілому в сфері національної безпеки і оборони, що пов'язано із оприлюдненням відповідної інформації. Повинно бути визначено форму, порядок та зміст звітування, терміни подання та строки звітування, процедури інформування про діяльність державних органів (наприклад, розміщення у форматі «відкриті дані»), а також наявність відповідних владних повноважень у адресатів звітування (Верховної Ради України, її Комітетів або спеціальних комісій) щодо реагування за наслідками звітування.

УДК: 341: 343.34: 316.774

Забара І.М.
кандидат юридичних наук, доцент,
Київський національний університет
імені Тараса Шевченка

КІБЕРНЕТИЧНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ: ДО ПИТАННЯ ВИЗНАЧЕННЯ НАПРЯМКІВ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ

Інформаційно-комунікаційні технології стрімко розвиваються, посилюючі вплив на ключові сфери діяльності держави. Враховуючи постійне розширення спектру використання цих технологій у кримінальних, терористичних і військових (військово-політичних) цілях, провідні країни світу впродовж десятиліть активно формують і вдосконалюють власні сектори безпеки.

Одним із важливих складових елементів виступає кібернетична безпека, що передбачає постійне і наполегливе впровадження новітніх алгоритмів та технології захисту інформації. Вагомим є й те, що при цьому враховуються економічні, політичні, технологічні, правові та інші можливості держав.

Питання кібернетичної безпеки має кілька напрямків розвитку. І, як правило, вони мають, серед іншого, правову основу і відповідне національне і, у певних випадках, міжнародно-правове регулювання.

Вагомими серед загроз, які охоплюють і визначають об'єкти, на захист яких повинні спрямовуватись намагання кібернетичного захисту, виступають:

- використання інформаційно-комунікаційних технологій для здійснення ворожих дій та актів агресії, а також на шкоду основним правам і свободам людини;

- цілеспрямований деструктивний вплив на критично важливі структури інших держав (в тому числі інформацію і інформаційні ресурси, елементи інфраструктури, програмне забезпечення, засоби і комплекси зв'язку, технологічні процеси тощо);

- дії в кібернетичному просторі з метою дестабілізації політичної, економічної і соціальної системи іншої держави;

- створення умов технологічної залежності у сфері інформаційно-комунікаційних технологій та інші.

Вважаємо, що крім зазначених, одним із майбутніх випробувань кібернетичних систем безпеки держав, вірогідно, буде відбуватись з боку штучного інтелекту.

У зв'язку з чим актуальними можуть виступити наступні питання: 1) що впливатиме на кібернетичні системи безпеки держав в нових умовах?; 2) на що саме впливатиме?; 3) які першочергові питання повинні бути вирішені для запобігання такому впливу?; 4) які можуть бути напрямки правового (міжнародно-правового) регулювання?

Вважаємо, що вплив на кібернетичні системи безпеки держав будуть здійснювати кілька чинників, серед яких: а) кількість кінцевих пристроїв, що отримуватимуть найрізноманітнішу інформацію (прогнозовано – 1 млн. кінцевих пристроїв на 1 кв. км); б) нові засоби і способи швидкісної передачі інформації (LiFI, квантовий зв'язок); в) засоби і технології, що працюватимуть із гігантськими обсягами зібраної, переданої і отриманої інформації (Super Data Base).

Здійснення впливу відбуватиметься на управління державою в цілому (управлінські рішення на рівні держави).

Серед першочергових питань, що повинні бути вирішені для запобігання такому впливу:

- яка інформація стане пріоритетною для запобігання її збиранню з нашої території (не тільки з баз даних, але й з території держави)?

- як контролювати потоки інформації, що збиратимуться на постійній основі гігантськими обсягами з нашої території?

- як впливати на масштабні потоки інформації, які пасивно вводитимуться на нашу територію?

- як впливати на масштабні потоки інформації, які цілеспрямовано вводитимуться на нашу територію?

- якими є вірогідні впливи на алгоритми та технології захисту інформації в умовах поширення технологій штучного інтелекту?

Вважаємо, що для України, актуальним напрямками міжнародно-правового регулювання постануть:

- укладення двосторонніх, регіональних і універсальних міжнародних угод з інформаційної і кібернетичної безпеки;

(варіант з укладенням універсальної міжнародної угоди (кількох угод) – на сьогодні - проблематичний і малоймовірний, враховуючи тривалу і не результативну діяльність Групи урядових експертів з інформаційної безпеки ООН, на яку покладено, серед інших, і розробку проекту угоди);

- входження до систем колективної безпеки, що передбачатиме спільні плани і заходи [1]; цей варіант – вірогідний, потребуватиме укладання окремої угоди (кількох угод) з міжнародною організацією. У разі, якщо вступ до такої (регіональної або універсальної) організації потребуватиме проходження тривалої процедури, це може стати альтернативним варіантом, що сприятиме забезпеченню кібернетичної безпеки держави в умовах масового впровадження і використання технологій штучного інтелекту.

Література

1. Забара І.М. Формування сучасних правових засад кібернетичної безпеки Європейського Союзу в умовах поширення нових інноваційних технологій / І.М. Забара // Журнал порівняльного і європейського права. – 2017, - №3. – С. 1-12.

УДК 341.824:338.47 (043.2)

Зайцев О.В.
Воєнно-дипломатична академія
імені Євгенія Березняка

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ – ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Актуальність проблеми забезпечення кібернетичної безпеки держави визначається наступними чинниками: різким збільшенням кількості кібернетичних атак з боку РФ, активізація співпраці Україна – НАТО в напрямку забезпечення кібернетичної безпеки, наявність на ринку широкого спектру технологій на програм підготовки з питань тестування на проникнення в кібернетичному просторі.

Серед найбільш руйнівних кібернетичних операцій проти України слід відмітити: операція "Змія", атака на "Вибори", атаки на енергетичні компанії України, операція "9 травня", операція "Прикормка", злам "Першого каналу", блокування роботи Держказначейства України, Компрометація ArtOS.

Тестування на проникнення (PENTEST) – це важлива складова заходів захисту об’єктів критичної інфраструктури технічного та організаційного характеру, що призначена для виявлення проблем в системі захисту об’єктів та, як наслідок, превентивного попередження кібернетичних атак в майбутньому. Тестування на проникнення здійснюється шляхом імітування кібернетичних акати на об’єкти захисту.

В доповіді наведено деякі приклади тестування на проникнення: впровадження програмних засобів типу вірус, троянський кінь, черв’як, маючи на меті компрометацію якомога більшої кількості систем; використання "ботнет" (мережі скомпрометованих комп’ютерів) для організації розподілених атак на відмову в обслуговуванні (DDOS); “таргетована атака" для тестування комп’ютерів установи або конкретних користувачів що перевіряються.

В доповіді розглядаються основні технології та програмні засоби для здійснення тестування на проникнення, серед яких слід виділити наступні: Nmap, Ettercap, WireShark, Flexera, W3af, Acunetix, BackTrack, Kali Linux, Retina, Arachoi, Core Impact, AirCrack-NG, BeEF, IronWASP, OpenVAS, Metasploit, Nessus, JohnTheRipper, PortsWigger, Peterva Maltego, Nagios, Canvas, Veracode, SqlMap, SqlNinja, RietSparker, Shodan та інші.

Досліджено сучасні методики проведення тестування на проникнення: Kill Chain, EY life cycle та інше. Визначений типовий алгоритм проведення тестування на проникнення: попередній збір інформації, дорозвідка цілей, ініціалізація атаки, здійснення атакуючих дій, підвищення рівня доступу, добування та передача інформації, знищення слідів роботи та закріплення в мережі для проведення подальших заходів.

Визначено, що важливою складовою тестування на проникнення є підготовка фахівців. Така підготовка повинна базуватись на матеріалах вже відомих курсів та тренінгів (в тому числі дистанційного навчання) типу Network Penetration Testing та Ethical Hacking таких провідних компаній як Offensive security, binsec, SANS, Udemy, EC-Council, CYBRARY, EH Academy.

Типова програма складається з інтенсивного тижневого (двотижневого) курсу підготовки та охоплює питання:

планування, визначення правил обмежень, рекогносцирування – збір загальнодоступної інформації (OSINT);

сканування доступних мереж (в тому числі бездротових типу Wi-Fi) з використанням програмних засобів типу Kali Linux (Aircrack--ng, John The Ripper, coWPAtty, Pyrit, Airdecap--ng, Kismet, Karmetasploit);

сканування локальних мереж (програмні засоби типу Tcpdump, Nmap, Nessus, Scapy, Netcat);

визначення та експлуатація вразливостей (програмні засоби типу Metasploit, Meterpreter, Armitage, Veil Framework, PowerShell);

проведення парольних атак (THC-Hydra, Metasploit Psexec, Hash Dumping, Metasploit Pivoting, Mimikatz Kiwi, John the Ripper, Cain, Hashcat);

проведення атак на мережні та Веб- сервіси (Nikto, ZAP Proxy, Cross-Site Request Forgery Vulnerabilities, Cross-Site Scripting Flaws, Command Injection Flaws, SQL Injection Flaws).

Література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.07.94 № 80/94-ВР // База даних «Законодавство України / ВР України». URL: http://zakon3.rada.gov.ua/laws/show/80/94-вр (дата звернення 04.03.2019).

2. Закон України Про основні засади забезпечення кібербезпеки України (Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403).

3. Закон України Про національну безпеку України (Відомості Верховної Ради (ВВР), 2018, № 31, ст. 241).

4. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України".

5. Конвенція про кіберзлочинність Статус Конвенції див. (994_789) {Додатковий протокол від 28.01.2003 до Конвенції див. (994_687)} (Конвенцію ратифіковано із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, № 5-6, ст. 71).

УДК 342.9(477)

Климчук О.О.
кандидат юридичних наук, доцент,
Національна академія Служби безпеки України
Тарасюк А.В.
кандидат юридичних наук,
Служба безпеки України

НОВАЦІЇ У СФЕРІ КІБЕРБЕЗПЕКИ ВЕЛИКОЇ БРИТАНІЇ

Великобританія входить до числа лідерів в області цифрових технологій. Значною мірою добробут країни залежить від здатності захистити технології, дані і мережі від загроз, що стоять перед суспільством. Кібератаки стають більш масовими, витонченими і мають руйнівні наслідки у разі успішного здійснення. Тому керівництво країни приймає рішучі заходи для захисту економіки і недоторканності приватного життя громадян Великобританії.

Нова Національна стратегія кібербезпеки Великої Британії (National Cyber Security Strategy 2016-2021) [1] становить собою рамкову програму

дій, направлених на зміцнення національної кібербезпеки, а також підвищення надійності і життєстійкості британського кіберпростору в найближчі роки.

У Національній стратегії кібербезпеки викладено план з перетворення Великобританії в державу, здатну впевнено протистояти загрозам в умовах швидкого розвитку цифрових технологій. Протягом п'ятирічного періоду дії стратегії планується вкласти 1,9 млрд фунтів стерлінгів у захист систем і інфраструктури, стримування супротивників і нарощування відповідного потенціалу в масштабах всього суспільства - від найбільших компаній до окремих громадян. Пропонується комплексний підхід до кібербезпеки, починаючи з елементарних правил безпеки і закінчуючи самими витонченими методами стримування загроз. Метою Стратегії є те, щоб атаки на будь-які об'єкти в Великобританії дорого обходилися зловмисникам. З цією метою уряд планує як зміцнювати оборону, так і розвивати кадровий потенціал в галузі кібернетики.

На підтримку Національної стратегії кібербезпеки у лютому 2019 року уряд Великобританії оголосив про нову стратегію експорту кібербезпеки. Вона допоможе британським компаніям в області кібербезпеки виграти контракти, які забезпечать безпеку для високопоставлених міжнародних покупців і захистять мережі по всьому світу. Ця нова стратегія була розроблена в промисловості і має надійні режими експортного контролю, які будуть захищати права людини.

Також у Великій Британії зроблено значний крок у сфері кібероборони - з ініціативи британського Міністерства оборони і Центру урядового зв'язку з'явиться новий вид військ – кібервійська, які будуть налічувати до двох тисяч осіб. А на фінансування нового підрозділу виділять понад 250 мільйонів фунтів стерлінгів.

Посилення кібервійськ є пріоритетним питанням для Великобританії в нинішніх умовах. Зосередженість на наступальних операціях дозволить забезпечити нові способи стримування і покарання держав, які бажають заподіяти шкоду країні[2].

Таким чином, можемо говорити про комплексний підхід до забезпечення кібербезпеки у Великобританії – окрім прийняття стратегічних документів у зазначеній сфері, здійснюються конкретні кроки з їх реалізації, зокрема, передбачено обсяг їх фінансування, розвиваються напрями, дотичні до кібербезпеки та пов'язані з нею (зокрема, експортна політика країни), створюються структури, відповідальні за реалізацію конкретних напрямів кібербезпеки.

Література

1. NationalCyberSecurityStrategy 2016-2021 // https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

2. Лондон створить нові кібервійська через загрози Росії – SkyNews // ttps://www.radiosvoboda.org/a/news-britain-kiberviyska/29501917.html.

УДК 161.15 + 007
Козубцов І.М.
кандидат технічних наук, професор РАЕ
Куцаєв В.В.
Козубцова Л.М.
Терещенко Т.П.
Військовий інститут телекомунікацій
та інформатизації імені Героїв Крут

ТЛУМАЧЕННЯ ТЕРМІНУ "КІБЕРНЕТИЧНА БЕЗПЕКА" ЧЕРЕЗ ПРИЗМУ КІБЕРНЕТИКИ

Постановка завдання. Використання у найрізноманітніших сферах життєдіяльності соціуму комп'ютерних і телекомунікаційних технологій, разом з великою кількістю переваг, привнесло також і чималу кількість загроз у цій сфері а саме проблему недоторканості та достовірності інформації. Реалізація цього роду загроз завдає значної шкоди функціонуванню інформаційно-інформаційних систем (ІТС), які використовують сучасні цифрові технології. Це привело до розуміння необхідності нейтралізації або мінімізації цієї сукупності загроз. Одночасно з цим виникає осучаснений термін "кібернетична безпека" якій і досі толком не осмислено.

Аналіз досліджень і публікацій. В контексті цього дослідження цікавим є тлумачення "кібербезпека" у документах Німеччини, Франції, Туреччини, Австралії [1].

Мета доповіді. По новому переосмислити тлумачення терміну "кібернетична безпека" через призму кібернетики.

Результат дослідження. В якості призми кібернетики будемо використовувати визначення [2]. Виходячи з цільового призначення систем, що містять в якості складових комп'ютерні системи та телекомунікаційні мережі, можна тлумачити, що кіберзагрози насамперед спрямовані на порушення циркуляції інформації [1]. Це поширена помилка розуміння кіберзагроз, оскільки це є наслідок дії кібернетичної загрози на комп'ютерні системи та телекомунікаційні мережі. Метою кібернетичної загрози (атаки) є саме вплив на управляючу складову ІТС, тобто на зміну алгоритму роботи систем.

Дійсно, кібернетичні загрози націлені на порушення власне обігу інформації на будь-якому з його етапів – створенні, поширенні, використанні, зберіганні і знищенні інформації. В сукупності з кінцевою метою на спотворення, недостовірність, несвоєчасність, несанкціоноване використання та поширення інформації з порушенням її цілісності та конфіденційності.

Наше припущення, що проблема кібербезпеки пов'язана з проблемою нейтралізації негативних інформаційних впливів на технологічному рівні на управління ІТС підтверджуються висновками з дослідження [1]. Части-

на цих проблем, наприклад, DDoS-атаки, виникають внаслідок обмеження технічних можливостей в управлінні ІТС, тобто не здатність управління ІТС справляються з обробкою шкідливого потоку завдань.

У випадку навмисного використання шкідливого програмного забезпечення типу (“троян”, “бекдор”, “вірус”, “руткіт”, “хробак” та ін.), з погляду кібернетики, це є втручання в алгоритми управління роботою ІТС в автономному режимі. Наслідком цього може бути знищення “кібернетичної безпеки” ІТС а саме її управління. Виходячи з цього, кібернетична загроза – це існування можливості реалізації деструктивного впливу на алгоритми управління “нормальною” роботою ІТС та її граничні технічні можливості (характеристики) з метою подальшого порушення циркуляції службової інформації та власне смислової інформації. Тоді “кібернетична безпека” – захищеність ІТС від деструктивних впливів на алгоритми управління роботою цієї системи.

Сформулюємо визначення “кібернетична безпека” на основі тлумачення дефініцій “Безпека”, яке запропоновано в роботі [3] з погляду кібернетики.

Приходимо к висновку, що “кібернетична безпека” ІТС, об’єкту, процесу, інформації тощо (чогось матеріального) – це такий стан і умови, в яких перебуває інформаційно-телекомунікаційний об’єкт захисту, коли кібернетичні дії (зовнішніх деструктивних факторів і внутрішніх чинників) не призводять до порушення нормального управління цього інформаційно-телекомунікаційного об’єкту, змін алгоритмів управління по відношенню до завдань інформаційно-телекомунікаційного об’єкту у відповідності до наявних на даному етапі потреб, знань та уявлень. Тоді “кібернетична безпека” об’єкту – це такий стан об’єкту, коли кібернетичні дії не призводять до порушення алгоритмів функціонування та управління об’єктом по відношенню до його завдань.

У швидкозростаючому інформаційному хаосі концепцій, доктрин, стратегій, програм, законів можна констатувати – фрагментарні, не вивчені, деколи суперечливі, не співставленні та не взаємопов’язані уявлення людства з відсутністю колективної інтелектуальної взаємодії. Яскравим прикладом цьому є Указ Президента України [4], в якому відсутнє офіційне державне тлумачення терміну “кібернетична безпека”. Спроба була зроблена у проекті Закону “Про кібернетичну безпеку України” [5], але даний закон не прийнятий.

Висновки. Отже: досі відсутнє чітке тлумачення терміну “кібернетичної безпеки”. На підставі кібернетичного підходу запропоновано тлумачення терміну “кібернетичної безпеки” через призму науки кібернетики, що дозволяє усунути імпліцитне уявлення, вихолощувати зайве та продовжити розбудову терміну “кібернетична безпека”.

Література

1. Баранов О.А. Про тлумачення та визначення поняття “кібербезпека” // Правова інформатика. – 2014. – № 2(42). – С. 54 – 62.

2. Словарь по кибернетике / Под ред. В.С. Михалевича. 2-е. К.: Главная редакция Украинской Советской Энциклопедии им. М.П. Бажана, 1989. С. 259.

3. Заплатинський В.М. Логіко-детермінантні підходи до розуміння поняття “Безпека”. Вісник Кам’янець-Подільського нац. ун-ту ім. І.Огієнка. Фізичне виховання, спорт і здоров’я людини. – 2012. – Вип. 5. – С. 90-98.

4. Указ Президента України “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" від 15.03.2016 № 96/2016.

5. Проект Закону про кібернетичну безпеку України [Електронний ресурс] // Верховна Рада України. Режим доступу URL: http://w1.c1.rada.gov.ua/pls zweb2/webproc4_1?pf3511=47240.

УДК [001.8/.816/.817] + 001.92 + [371.315.5/.315.6/.335] +655.52

Козубцов І.М.
кандидат технічних наук, професор РАЕ
Куцаєв В.В.
Козубцова Л.М.
Терещенко Т.П.
Штонда Р.М.
Військовий інститут телекомунікацій
та інформатизації імені Героїв Крут

КІБЕРНЕТИЧНІ АТАКИ ЯК МЕХАНІЗМ СТВОРЕННЯ ШТУЧНОГО ГЛОБАЛЬНОГО КОЛАПСУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Постановка завдання. У зв’язку із збільшення обсягу обміну інформації в інформаційно-телекомунікаційних мережах, в тому числі і в мережах спеціального призначення, збільшується ризик додаткового навантаження на мережі, що призводить до перевантаження та значного зменшення пропускної здатності мережі, аж до виникнення колапсу, результатом якого є втрата інформації. В зв’язку з цим важливо усвідомити механізм пошуку шляхів протидії можливому штучному створенню глобального колапсу інформаційно-телекомунікаційних систем”.

Мета доповіді є усвідомлення механізму створення штучного глобального колапсу інформаційно-телекомунікаційних систем (ІТС).

Результат дослідження. Перш ніж розглянути механізм можливого створення штучно колапсу інформаційно-телекомунікаційних систем слід уяснити поняття “Глобальний колапс ІТС”, що містить складові “ГЛОБАЛЬНИЙ” + “КОЛАПС” + “ІНФОРМАЦІЙНО-

ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ” і пропонуємо, трактувати як настання глобальних наслідків планетарного значення техногенного, технологічного, економічного або військового характеру в наслідок деструктивного кібернетичного впливу, націленого на руйнування технологічних процесів (алгоритмів) нормального функціонування ІТС (сукупності ІТС) та мережі, в результаті чого порушується інформаційна безпека, а саме здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації.

Механізм можливого штучно створеного колапсу ІТС витікає із огляду вразливостей функціонування ІТС, які в сукупності об’єднують інформаційні (комп’ютерні) та телекомунікаційні системи. Згідно Закон України “Про телекомунікації” ключовою загрозою в ІТС та мережах є забезпечення інформаційної безпеки.

Ключова мета навмисних деструктивних впливів на технологічно-управляючу підсистему для порушення алгоритму її “нормальної” роботи є створення колапсу в ІТС, тобто порушення інформаційної безпеки. Такою силою деструктивного впливу, з сучасної практики, є кібернетичні загрози (атаки). Найчастіше джерелом деструктивного кібернетичного впливу є різного налаштування та мотивації групи осіб, які культивують культ “Хакера”. Такі загроз можуть надходити і від кримінального елементу, а уразі позитивного впливу на мотиваційні характеристики військовослужбовця можна переманити на зацікавлену сторону кібернетичного протистояння [1].

Результативно, кібернетичні загрози різним шляхом націлені порушити власне обіг інформації на будь-якому з його етапів – створенні, поширенні, використанні, зберіганні і знищенні інформації, а в сукупності з кінцевою метою на спотворення, недостовірність, несвоєчасність, несанкціоноване використання та поширенням інформації, порушенням її цілісності та конфіденційності.

Частина цих проблем виникає через *DDos*-атаки, внаслідок кінцевої границі технічних можливостей комп’ютерних систем з обробки запитів та обмеженість пропускної здатності лінії волоконно-оптичних каналів зв’язку.

У випадку навмисного використання шкідливого програмного забезпечення типу (“троян”, “бекдор”, “вірус”, “руткіт”, “хробак” та ін.), з погляду кібернетики, це є втручання в алгоритми управління роботою ІТС в автономному режимі. Наслідком цього може бути знищення “кібернетичної безпеки” ІТС а саме її управління. Виходячи з цього, кібернетична загроза – це існування можливості реалізації деструктивного впливу на алгоритми управління “нормальною” роботою ІТС та її граничні технічні можливості (характеристики) з метою подальшого порушення циркуляції службової інформації та власне смислової інформації.

Вразливими елементами ІТС є: інформаційні (комп'ютерні) системи; стаціонарні і мобільні комп'ютери операторів, інженерів та звичайних користувачів; сервери, зокрема сервери віртуалізації, на яких встановлено ПЗ моніторингу і управління технологічним процесом; мережеві маршрутизатори; шлюзи даних; контролери; модеми; мережеві адаптери; концентратори; мультиплексори; польові промислові пристрої різного ступеня "інтелектуальності" з цифровим (характерний для сучасніших пристроїв) або аналоговим інтерфейсом комунікації; програно-апаратні firewall; комутатори.

Ці елементи є критично важливими, оскільки з них будується ІТС та мережі. Тому їх необхідно захищати від кібернетичного впливу.

Висновки. Таким чином, глобальний колапс інформаційно-телекомунікаційних систем може бути реалізовано, наприклад шляхом реалізації кібернетичні атаки на цю систему або систему керування електрогенеруючих компаній з метою безструмлення обладнання.

Література

1. Козубцов І.М., Козубцова Л.М., Живило Є.О., Куцаєв В.В. Про необхідність дослідження мотиваційної характеристики військовослужбовців при допуску їх до кібернетичного протистояння // Науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" (17-18 березня 2016 р., м. Харків). – Харків: НАНГУ, 2016. С.35-36.

УДК 004.7(075)

Гордієнко С.Б.
кандидат технічних наук, доцент
Козюра В.Д.
кандидат технічних наук, доцент,
Національна академія Служби безпеки України

ПРОБЛЕМИ IP-АДРЕСАЦІЇ

Основу міжмережевої взаємодії локальних комп'ютерних мереж складає IP-адресація, що реалізовується стеком протоколів TCP/IP. Обмеженість версії IPv4 у зв'язку з колосальною динамікою зростання кількості хостів в Інтернеті вимагає реалізації нових підходів до організації адресації [1]. Метою дослідження є висвітлення проблем, пов'язаних з IP-адресацією.

IP-адреса – це унікальний числовий адрес, що однозначно ідентифікує вузол, групу вузлів або комп'ютерну мережу і має довжину 4 байти, наприклад, 213.128.193.154.

IP адресація – це процес розподілу IP-адрес в середині мережі або підмережі, що підтримують стек протоколів TCP/IP, і реалізовується вручну (адреси розподіляє адміністратор) чи автоматизовано (наприклад, через протокол розподілу DHCP).

Стек TCP/IP – систематизований набір протоколів мережі Інтернет, що поділяється на чотири рівні, які корелюються з еталонною моделлю OSI. В зв'язці зі стеком використовуються три типи адрес: локальні (апаратні), IP-адреси й символьні доменні імена.

В залежності від розмірів мережі кількість адрес може бути більшою або меншою. Для різних потреб існує кілька класів мереж [2-5]:

- Class A – включає мережі з адресами 1.0.0.0 до 127.0.0.0 (номер мережі знаходиться в першому байті октету, що забезпечує 24-ох розрядну частину для означення хостів – дозволяє використання приблизно 16 мільйонів хостів у мережі);
- Class B – включає мережі з адресами 128.0.0.0 по 191.255.0.0 (номер мережі знаходиться в перших двох байтах октету. Це нараховує 16320 мереж з 65024 хостом у кожній);
- Class C – діапазон мереж від 192.0.0.0 по 223.255.255.0 (номер мережі — перших три числа в октеті. Нараховує 2 мільйони мереж з 254 хостами в кожній);
- Class D, E, та F – адреси, що підпадають в діапазон з 224.0.0.0 по 254.0.0.0 є або експериментальними, або збережені для використання у майбутньому і не описують жодної мережі.

Але для сприйняття користувачем IP-адреса незручна. Людині краще працювати з іменами. Тому користувачі звичайно працюють із доменними адресами – унікальними іменами комп'ютерів у Internet. Доменна адреса, так само як і IP-адреса, складається з частин, розділених крапками. Але на відміну від IP-адреси, що уточнює місце призначення зліва направо, доменна адреса робить це у зворотному порядку – справа наліво: спочатку йде ім'я комп'ютера, а потім – ім'я мережі, в якій він знаходиться.

Номера мереж призначаються або централізовано, якщо мережа є частиною Інтернет, або довільно, якщо мережа працює автономно (для локальних мереж).

Стрімке зростання Інтернету привело до дефіциту IP-адрес. Дуже важко одержати адресу класу B и практично неможливо стати власником адреси класу A. При цьому слід відзначити, що дефіцит обумовлений не тільки ростом мереж, але й тим, що наявна безліч IP-адрес використовується нераціонально. Дуже часто власники мережі класу C витрачають лише невелику частину з наявних у них 254 адрес. Якщо ж деяка IP-мережа створена для роботи в «автономному режимі», без зв'язку з Інтернет, тоді адміністратор вільний призначити їй довільно обраний номер. Але у цій ситуації для того, щоб уникнути яких-небудь колізій, у стандар-

тах Інтернет визначено кілька діапазонів адрес, що рекомендують для локального використання: у класі А – це мережа 10.0.0.0, у класі В – це діапазон з 16 номерів мереж 172.16.0.0 – 172.31.0.0, у класі С – це діапазон з 255 мереж – 192.168.0.0 – 192.168.255.0 (ці адреси не обробляються маршрутизаторами ні при яких умовах).

Для зм'якшення проблеми дефіциту адрес пропонуються різні підходи:

- перехід на нову версію IP-протоколу – IPv6, у якому різко розширюється адресний простір за рахунок використання 16-байтних адрес;
- використання технології масок й її розвитку – технології безкласової міждоменної маршрутизації (Classless Inter-Domain Routing, CIDR) [4, 5] – у рамках. поточної версії IPv4. Ця технологія відмовляється від традиційної концепції розподілу адрес протоколу IP на класи, що дозволяє отримувати в користування стільки адрес, скільки реально необхідно. Постачальник послуг дістає можливість «нарізати» блоки з виділеного йому адресного простору в точній відповідності з вимогами кожного клієнта, при цьому в нього залишається простір для маневру на випадок майбутнього зростання;
- використання технології трансляція адрес (Network Address Translator, NAT) [4]. Вузлам внутрішньої мережі адреси призначаються довільно. Внутрішня мережа з'єднується з Інтернет через деякий проміжний пристрій (маршрутизатор, міжмережевий екран, прокси-сервер), який отримує у своє розпорядження деяку кількість зовнішніх «нормальних» IP-адрес, погоджених з постачальником послуг, і здатний перетворювати внутрішні адреси в зовнішні, використовуючи для цього таблиці відповідності. Для зовнішніх користувачів всі численні вузли внутрішньої мережі виступають під декількома зовнішніми IP-адресами. При одержанні зовнішнього запиту цей пристрій аналізує його вміст і при необхідності пересилає його у внутрішню мережу, заміняючи IP-адресу на внутрішню адресу необхідного вузла. Процедура трансляції адрес визначена в RFC 1631.

NAT – перетворення (трансляція) мережних адрес – це механізм зміни мережної адреси в заголовках IP датаграм, поки вони проходять через маршрутизуючий пристрій з метою відображення одного адресного простору в інший.

Перетворення адрес методом NAT може здійснюватись практично будь-яким пристроєм маршрутизації – маршрутизатором, сервером доступу, міжмережевим екраном. Завдяки NAT можна, використовуючи одну або кілька зовнішніх IP-адрес, виданих провайдером, підключити до мережі практично будь-яку кількість комп'ютерів.

PAT (Port Address Translation) – це можливість мережевих пристроїв, яка транслює TCP або UDP зв'язки, встановлені між хостами в приватній мережі та хостами в публічній мережі. Вона дає можливість одиничній

публічній IP-адресі бути використаною багатьма хостами в приватній мережі.

Висновки. Вирішення проблеми дефіциту мережевих адрес можливо декількома шляхами: 1) перехід на нову версію протоколу IPv6, яка зажадає значних технічних і фінансових витрат; 2) використання технології безкласової міждоменної маршрутизації CIDR; 3) використання технології трансляція адрес NAT і PAT. Останні два підходи дозволяють у рамках діючого протоколу IPv4 значною мірою ослабити проблему дефіциту.

Література

1. Современные тенденции развития телекоммуникационных сетей. [Електронний ресурс]. – Режим доступу: http://sernam.ru/book_history.php?id=25.

2. Класифікація IP-адрес. [Електронний ресурс]. – Режим доступу: https://studopedia.su/17_17340_klasifikatsiya-IP-adres.html. -

3. Порядок розподілу IP-адрес. [Електронний ресурс]. – Режим доступу: http://www.matveev.kiev.ua/archnet/gl5/012.htm.

4. Принципи трансляції мережевих адрес. [Електронний ресурс]. – Режим доступу: http://um.co.ua/9/9-16/9-169782.html.

5. Основы компьютерных сетей. IP-адресация. [Електронний ресурс]. – Режим доступу: http://net.e-publish.ru/p234aa1.html.

УДК 347.734

Іванов Ю.А.
кандидат юридичних наук, доцент,
Національна академія Служби безпеки України

АКТУАЛЬНІ ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В КРЕДИТНО-БАНКІВСЬКІЙ СФЕРІ

Законодавство України щодо захисту критичної інфраструктури, в тому числі, у кредитно-банківській сфері перебуває на етапі становлення. При цьому в умовах розвитку сучасного інформаційного суспільства першочерговим завданням є побудова адекватної викликам сьогодення системи протидії кіберзагрозам.

Роль НБУ у системі кіберзахисту критичної інфраструктури у кредитно-банківській сфері обумовлена його специфічним подвійним правовим статусом. Як орган державного управління він є одним із ключових суб'єктів, котрі мають забезпечувати функціонування системи кіберзахисту у кредитно-банківській сфері. Водночас, будучи банком, НБУ здійснює банківську діяльність (хоч і зі значними особливостями, що вирізняють його з-поміж інших банків) і тому сам підлягає захисту.

У сфері забезпечення інформаційної безпеки та кіберзахисту на теренах України послідовно втілюється європейська концепція захисту критичної інфраструктури. Значущою подією у цьому контексті слід визнати прийняття Закону України «Про основні засади забезпечення кібербезпеки України» [1]. Цим законом, серед іншого, внесено зміни до Закону України «Про Національний банк України» [2], які стосуються закріплення за регулятором додаткових функцій, одна з яких полягає у тому, що відтепер НБУ має визначати порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснювати контроль за їх виконанням, утворити центр кіберзахисту НБУ і у цілому забезпечувати функціонування системи кіберзахисту у банківській системі. Друга із цих функцій виходить за межі виключно інформаційної безпеки та кіберзахисту й полягає у забезпеченні формування та ведення переліку об'єктів критичної інфраструктури, а також реєстру об'єктів критичної інформаційної інфраструктури у банківській системі, визначенні критеріїв та порядку віднесення об'єктів банківської системи до об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, забезпеченні оцінювання стану кіберзахисту та аудиту інформаційної безпеки у банківській системі.

Слід зазначити, що вказані функції неможна охарактеризувати як принципово нові для НБУ, адже питання інформаційної безпеки вже протягом тривалого часу були серед пріоритетів його регулятивної та наглядової діяльності. Але, безперечно, оформлення цих напрямів діяльності регулятора у якості окремих функцій є цілком адекватним потребам сьогодення, коли кіберзагрози стали одним із ключових чинників, котрі негативно впливають на банківську безпеку. За таких умов вкрай важливим практичним кроком щодо імплементації положень оновленого законодавства стало створення Центру кіберзахисту НБУ.

Проблеми кіберзахисту з особливою гостротою постали в умовах воєнного стану, який був введений в Україні наприкінці 2018 р. У зв'язку з цим НБУ Листом від 03.12.2018 р. № 56-0007/64280 «Щодо посилення кіберзахисту банківської системи України» зорієнтував банки щодо дій, які варто вчинити для підтримання необхідного рівня кіберзахисту та кібербезпеки в банківській системі в принципово нових нестандартних умовах. При цьому було запропоновано терміново інформувати новостворений Центр кіберзахисту НБУ про виявлені кібератаки, котрі спроможні або взагалі унеможливити виконання відповідних банківських операцій, або значною мірою ускладнити діяльність банку чи банківської системи загалом. Такі дії регулятора були абсолютно доречними, позаяк воєнний стан було запроваджено вперше в історії незалежної України і тому надання відповідних роз'яснень, крім суто юридичного значення, мало ще психо-

логічний ефект. Водночас звертає на себе те, що текст листа сформульовано за допомогою мовностилістичних засобів, які свідчать про не зобов'язуючий, а суто рекомендаційний характер його змісту. Це пояснюється тим, що листи НБУ є лише документами інформаційно-аналітичного спрямування, а не різновидом нормативно-правових актів. Тому їх зміст, як правило, зводиться до певних роз'яснень, нагадувань, узагальнень.

У подальшому порядок взаємодії банків з Центром кіберзахисту НБУ необхідно якнайшвидше закріпити нормативно. Поряд з цим, для забезпечення належної реалізації вище окреслених відносно нових для НБУ функцій необхідно прийняти низку нормативно-правових актів, які регламентуватимуть комплекс питань, що стосуються інформаційної безпеки й кіберзахисту банківської системи, а також об'єктів критичної інфраструктури та критичної інформаційної інфраструктури у її складі.

Розбудова системи інформаційної безпеки та кіберзахисту має супроводжуватись загальним вдосконаленням механізмів банківського регулювання та нагляду з урахуванням європейських стандартів та відповідних положень Угоди про асоціацію між Україною та ЄС [3].

Література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII / Верховна Рада України. Відомості Верховної Ради України. 2017. №45. Ст. 403.

2. Про Національний банк України: Закон України від 20 травня 1999 р. № 679-XIV / Верховна Рада України. Відомості Верховної Ради України. 1999. № 29. Ст. 238.

3. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом і його державами-членами, з іншої сторони. // Урядовий портал. URL: http://www.kmu.gov.ua/ (дата звернення: 28.02.2019).

УДК 343.98

Корнейко О.В.
кандидат технічних наук, професор
Школьніков В.І.
Національна академія внутрішніх справ

ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Компанія ThreatMetrix оприлюднила дані, що свідчать про збільшення обсягів кібератак на 30 % в Європі впродовж першого кварталу 2018 року [1]. Оскільки світ стає більш цифровим, кібератаки стають більш складними, то відповідно матеріально-технічне забезпечення правоохоронних органів повинно відповідати сучасним реаліям суспільного життя.

На жаль, слід відмітити недостатній рівень забезпечення правоохоронних органів відповідним комп'ютерним оснащенням.

Проблему недостатнього матеріально-технічного забезпечення можливо вирішити за допомогою використання хмарних технологій, обслуговування яких як правило є дешевшим порівняно із обслуговуванням традиційних персональних комп'ютерів.

Перевагами використання такої технології є:

– необов'язкова наявність потужних персональних комп'ютерів;

– економія витрат на використання ліцензованого програмного забезпечення та його постійного оновлення;

– великий обсяг пам'яті для зберігання даних;

– відсутність прив'язки до робочого місця, тобто існує можливість доступу до хмарних обчислень з різних пристроїв;

– високий рівень захисту даних та можливість відновлення інформації в разі її знищення.

Хмарні технології (з англ. Cloud Technology) – це нова інформаційна парадигма, що передбачає віддалену обробку та зберігання даних. Характерною ознакою цієї технології є використання електронно-обчислювальних можливостей віддалених серверів, які розташовані по всьому світові. Тобто, не обов'язково мати персональний комп'ютер із високими характеристиками процесора, оперативної пам'яті, відеокарти тощо. Головною умовою є наявність швидкісного підключення до Інтернету.

Необхідно погодитися із думкою Шепітька В.Ю. про те, що інформаційні технології надають можливість оперативного збирання, зіставлення та аналізу відомостей з різних джерел (повідомлень, результатів оперативно-розшукових заходів, допитів, адресної бази даних тощо), установлення хронологічної послідовності подій за часом та відповідності окремих фактів, дозволяють здійснювати складання планів та схем місця події, моделювання події злочину за допомогою комп'ютерної техніки та ін. [2, с. 196-197].

На сьогодні такі сервіси як Amazon Web Services та Digital Ocean Cloud Servers надають можливість використовувати віртуальні комп'ютери.

Наприклад, Amazon Web Services надає в оренду інфраструктуру для хмарних обчислень приватним або юридичним особам на основі платної підписки. Існує також і безкоштовна підписка, яка доступна протягом перших 12 місяців.

Ця технологія дозволяє мати в розпорядженні повноцінний віртуальний кластер комп'ютерів, який завжди доступний через Інтернет. Віртуальні комп'ютери AWS мають більшість атрибутів реального комп'ютера, включаючи апаратні пристрої (процесор, відеокарту, локальну та оперативну пам'ять, жорсткий диск або SSD-накопичувач); операційну систему на вибір; мережу; і попередньо встановлені прикладні програми тощо.

Слід відмітити, що AWS надає різні операційні системи у користування, починаючи від Windows 2016, Windows 2012 R та закінчуючи Ubuntu, CentOS, Red Hat Enterprise Linux.

Тобто, сервіс AWS може замінити традиційний персональний комп'ютер та бути використаним в діяльності правоохоронних органів, але відповідно до вимог чинного законодавства в сфері технічного захисту інформації та охорони державної таємниці.

Крім закордонних сервісів, правоохоронні органи мають можливість використовувати вітчизняні дата-центри, наприклад «Парковий».

Слід відмітити, що на разі в Верховній Раді України зареєстрований законопроект № 4302 від 24.03.2016 «Про внесення змін до деяких законів України (щодо обробки інформації в системах хмарних обчислень)», який передбачає використання органами державної влади хмарних технологій для обробки інформації (крім інформації, яка в установленому порядку віднесена до державної таємниці).

Сучасний розвиток інформаційних технологій надає правоохоронним органам безліч можливостей у боротьбі із злочинністю. Використання хмарних технологій можуть значно зекономити час та ресурси. Єдиною перепоною цьому є законодавче врегулювання можливості використання хмарних технологій під час обробки інформації, що становить державну таємницю. Це зумовлює необхідність подальших наукових розробок щодо можливості використання хмарних технологій в діяльності правоохоронних органів.

Література

1. 2018 Cybercrime Report Europe Deepdive. URL: https://www.threatmetrix.com/info/2018-cybercrime-europe/ (дата звернення 04.03.2018).

2. Шепітько В.Ю. Інформаційні технології в криміналістиці та слідчій діяльності. Питання боротьби зі злочинністю. Харків, 2010. № 19. С. 194-202.

УДК 001.8

Кравець В.М.
кандидат технічних наук,
старший науковий співробітник,
Національна академія Служби безпеки України

ПОРІВНЯЛЬНИЙ АНАЛІЗ МІЖНАРОДНИХ ІНДЕКСІВ КІБЕРБЕЗПЕКИ

Ученими, аналітиками та фахівцями-практиками застосовуються різні показники та індекси для оцінки стану кібербезпеки залежно від об'єкта

захисту, цілей та завдань такої оцінки, рішень, які приймаються на їх основі. У даному дослідженні здійснюється порівняльний аналіз структури, методик формування та застосування найбільш відомих міжнародних індексів кібербезпеки (Глобального індексу кібербезпеки, Національного індексу кібербезпеки та Галузевого індексу кібербезпеки) з метою подальшого поширення практики їх використання в інтересах наукових та аналітичних досліджень.

Глобальний індекс кібербезпеки (Global Cybersecurity Index, GCI) - це надійна характеристика, яка на глобальному рівні вимірює, як уряди країн виконують зобов'язання із забезпечення кібербезпеки - для підвищення обізнаності про важливість і різні виміри проблеми [1]. Національний індекс кібербезпеки (National Cyber Security Index, NCSI) - це індекс, який на глобальному рівні оцінює готовність країн протидіяти кіберзагрозам та управляти кіберінцидентами. NCSI також є базою даних, яка містить загальнодоступні матеріали та засоби, які підтверджують здатність розбудовувати національну систему кібербезпеки [2]. Галузевий індекс кібербезпеки (Index of Cyber Security, ICS) - це показник ризику для корпоративної, промислової та урядової інформаційної інфраструктури, що базується на настроях фахівців-практиів, через спектр загроз кібербезпеки. Він ґрунтується на настроях у розумінні швидкої зміни загроз і станів кібербезпеки, розглядає систему метрик кібербезпеки як прикладне мистецтво, і залежить від ступеня невизначеності як у будь-якій ризикоорієнтованій сфері [3].

Узагальнена інформація наводиться у таблиці 1.

Таблиця 1

Порівняльний аналіз сучасних індексів кібербезпеки

	Global Cybersecurity Index, GCI	National Cyber Security Index, NCSI	Index of Cyber Security, ICS
Що вимірює?	Виконання урядами країн зобов'язань із забезпечення кібербезпеки	Готовність країн протидіяти кіберзагрозам та управляти кіберінцидентами	Ризик реалізації кіберзагроз для корпоративної, промислової та урядової інформаційної інфраструктури
Призначення	Розбудова міжнародної системи кібербезпеки, формування державної політики	Надання інформації про актуальний стан національної системи кібербезпеки певної країни, розбудова національної системи кібербезпеки	Управління ризиками кіберзагроз в конкретній організації, розробка нових продуктів безпеки, управління фінансовими ринками
Завдання	• Допомога країнам у визначенні секторів, які потребують удосконалення • Мотивація діяльності з удосконалення власного GCI рейтингу • Зростання рівня кібербезпеки у світі • Допомога у визначенні та просуванні найкращих практик • Формування глобальної культури кібербезпеки	• Отримання актуальної інформації про стан розвитку національних систем забезпечення кібербезпеки • Порівняння власного рівня розвитку системи кібербезпеки із системами інших країн • Поширення інформації про найкращі практики	• Оцінювання рівня ризику за досвідом фахівців-практиків у сфері кібербезпеки • Поширення загальної оцінки для більш широкого кола зацікавлених осіб • Порівняння власного досвіду та оцінки кіберзагроз із загальною оцінкою • Зростання рівня кібербезпеки організації
Оновлення	2014, 2017, формується наступна версія	постійно	щомісяця
Методи	Експертне оцінювання, багатокритеріальний аналіз, математичне зважування	Експертне оцінювання, лінійна функція	Експертне оцінювання, математичне зважування, аналіз часових рядів

Основні категорії	• Правові заходи • Технічні заходи • Організаційні заходи • Розбудова спроможності • Співпраця	• Загальні показники кібербезпеки (регулювання, освіта, обмін інформацією, міжнародна співпраця) • Базові показники кібербезпеки (захист основних сервісів) • Здатність управляти кіберінцидентами та кризовими ситуаціями (протидія у кіберпросторі)	• Суб'єкти атак • Засоби атак • Мета атак • Об'єкти атак • Уразливість засобів захисту • Загальне відчуття загроз
Кількість показників	• GCIv1 - 17 індикаторів 17 питань • GCIv2 - 25 індикаторів 157 питань • GCIv3 - 25 індикаторів 50 питань	46 індикаторів	25 індикаторів
Респонденти	Експерти державних установ та комерційних компаній, громадських організацій країни, що оцінюється; експерти міжнародних організацій	Офіційні представники уряду країни, що оцінюється, організація або приватна особа, експерти команди-розробника індексу	Відібрані особисто групою розробників фахівці-практики у сфері кібербезпеки (список не оприлюднюється)
Кількість країн	194 (надіслали первинні дані: GCIv1 - 105 країн GCIv2 – 134 країни)	126	-
Верифікація	Здійснюється експертами партнерських організацій	Здійснюється не менше, ніж двома експертами команди-розробника індексу	Не здійснюється
Розробники	МСЕ спільно з партнерськими організаціями	Академія електронного урядування (м. Таллін) спільно з партнерськими організаціями Естонії	Американські експерти у галузі комп'ютерної безпеки та управління ризиками Dan Geer та Mukul Pareek

Порівняльний аналіз сучасних міжнародних індексів кібербезпеки GCI, NCSI, ICS свідчить, що усі вони визначаються за результатами експертного оцінювання, але мають різне призначення: розбудова міжнародної системи кібербезпеки, надання інформації про актуальний стан національних систем кібербезпеки та управління ризиками кіберзагроз конкретної організації відповідно. Глобальний та національний індекси мають подібний пул респондентів, схожі за підходом до верифікації даних, але мають різні системи індикаторів та оцінювання. Глобальний індекс кібербезпеки більш повний та авторитетний, більш відомий. Водночас, національний - найбільш актуальний, точний та відображає поточний стан, а не ситуацію у минулому, хоча й найближчому. Крім цього, національний індекс є не статичною таблицею, а забезпечений сучасними програмними засобами (сервісами) для обробки даних. Глобальний та національний індекси є також більш надійними, завдяки верифікації даних. Верифікація галузевого індексу взагалі не здійснюється, але він унікальний тим, що оцінює не країни, а ризики (ймовірність появи загроз, активність певних суб'єктів кібератак, застосування тих, чи інших інструментів атак тощо).

Результати даного дослідження можуть бути використані для подальшого удосконалення інструментів аналізу даних, які характеризують стан кібернетичної безпеки у світі.

Література

1. Global Cybersecurity Index [Електронний ресурс] // International Telecommunication Union (ITU). - Режим доступу: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

2. National Cyber Security Index [Електронний ресурс] // e-Governance Academy. - Режим доступу: https://ncsi.ega.ee.

3. Index of Cyber Security [Електронний ресурс] / D. Geer, M. Pareek // Режим доступу: http://cybersecurityindex.org/index.php.

УДК 351.86(477)

Кушнір В.О.
кандидат наук з державного управління,
Національний університет оборони України
імені Івана Черняховського
Макарченко І.А.
Національний університет оборони України
імені Івана Черняховського

ІНФОРМАЦІЙНА БЕЗПЕКА ВІЙСЬКОВОСЛУЖБОВЦІВ В ІНТЕРНЕТІ ЯК ЧИННИК ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВІЙСЬКОВОЇ ОПЕРАЦІЇ

Збройні конфлікти третього тисячоліття характеризуються обширним висвітленням сцен бойових дій або так званим "ефектом присутності",

який досягається зйомками зіткнень між воюючими сторонами з різних ракурсів в режимі реального часу. Соціальні мережі в цьому контексті надають можливість їх користувачам бачити ті моменти бойових дій, які не можуть зняти навіть військові кореспонденти.

Недотримання заходів інформаційної безпеки під час користування інтернетом військовослужбовцями, залученими до військових операцій, впливало на хід усієї операції та у деяких випадках призводило до загибелі особового складу.

Невмілі користувачі соцмереж – цінне джерело інформації для зацікавлених осіб. Яскравим прикладом в цьому контексті є розслідування дослідницької пошукової мережі Bellingcat, в рамках яких розкрито численні факти агресії Росії: збиття російським ЗРК "Бук" літака Boeing 777 біля Донецька, ідентифікація осіб та підрозділів ЗС РФ, що брали участь в збройній агресії проти України, викриття осіб, причетних до отруєння колишнього співробітника ГРУ ЗС РФ О. Скрипаля тощо [1]. В розслідуваннях Bellingcat використовуються всі можливі види даних, від інформації про геолокацію, до фотографій та співставлення біографічних даних осіб з хронологією подій.

В свою чергу, інформація з соцмереж про військовослужбовців ЗС України та інших силових відомств також активно збирається російськими спецслужбами. Хакерська група "Берегині", яка пов'язана з РФ, містить масштабну базу даних з інформацією про українських військовослужбовців, які беруть участь в ООС та брали участь в АТО (місце служби, склад сім'ї, адреса проживання та ін. персональні дані), що становить загрозу безпеці військовослужбовців та членів їх сімей.

Іншим прикладом небезпеки використання Інтернет-додатків є інцидент з публікацією маршрутів пересування користувачів фітнес-додатку "Strava", в якому за маршрутом пересування американських військових у Сирії можна було визначити периметр їх військової бази [3]. В разі потрапляння цієї інформації до рук противника, під загрозу потрапляє не тільки операція, а й безпека всього підрозділу, а географічна прив'язка даних до інфраструктурних об'єктів стратегічної важливості може становити загрозу національній безпеці держави.

Останні два десятиліття в оборонних відомствах різних країн ведеться активна дискусія щодо використання військовослужбовцями соцмереж та можливих обмежень свободи в інформаційному просторі в цьому контексті [4]. З початку 2010 р. в ЗС багатьох країн були видані посібники з користування соцмережами для військовослужбовців, що ілюструє значимість ІТ та соцмереж у діяльності військ. В ЗС США були випущені посібники з користування соціальними мережами Сухопутними військами ЗС США (2011 рік) та Військово-морськими Силами (2018 року) [5].

З метою недопущення загроз безпеці військовослужбовців та успішності операцій, Кодекс Оборони Франції передбачає обмеження або заборону використання будь-яких засобів комунікації під час виконання бойових завдань [6]. В Королівських ЗС Канади обмеження на використання засобів комунікації, зокрема соцмереж, визначаються для кожної окремої операції [7]. В Королівських ЗС Великої Британії діє подібна до канадської політика стосовно використання соцмереж військовослужбовцями, проте використання соцмереж розділяється на три типи: особисте, офіційне, корпоративне. Обмеження щодо використання засобів комунікації та соцмереж визначаються для кожної окремої операції.

Враховуючи сучасну популярність соціальних мереж та присутність у них військовослужбовців ЗСУ, можливості OSINT-розвідки, слід відзначити ризики, які соцмережі представляють для безпеки військовослужбовців, їх сімей, безпеки операцій і, як наслідок, національної безпеки держави та розробити і впровадити політики, базовані на вже існуючому досвіді країн-членів Альянсу, щодо користування соціальним мережами військовослужбовців, що залучаються до військових операцій.

Література

1. Bellingcat. [Електронний ресурс]. – Режим доступу: https://www.bellingcat.com/.

2. Берегини. [Електронний ресурс]. – Режим доступу: https://bg14.org/.

3. The Guardian. Fitness-tracking app gives away location of secret US Army bases. [Електронний ресурс]. – Режим доступу: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

4. Office of the Chief of Public Affairs. U.S. Army Social Media Handbook. Pentagon, 2011.

5. Assemblée Nationale. Code de la defense. Article L4121-2, L4121-3. [Електронний ресурс]. – Режим доступу: https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9C90831DA5837CD5AA5DE4BF54997399.tplgfr28s_1?idArticle=LEGIARTI000006540242&cidTexte=LEGITEXT000006071307&dateTexte=20190304.

6. National Defence and the Canadian Armed Forces. DAOD 2008-8, Official Use of Social Media. [Електронний ресурс]. – Режим доступу: http://forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-2000/2008-8.page#op.

7. The British Army. Social Media Policy. [Електронний ресурс]. – Режим доступу: https://www.army.mod.uk/who-we-are/our-people/a-soldiers-values-and-standards/social-media-policy/.

УДК 355.233.21
Лагун А. Е.
кандидат технічних наук, доцент,
Львівський державний університет безпеки життєдіяльності

ОСОБЛИВОСТІ НАВЧАННЯ СТУДЕНТІВ ЗА СПЕЦІАЛЬНІСТЮ «КІБЕРБЕЗПЕКА» СПЕЦІАЛІЗАЦІЄЮ «УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ» У ЛЬВІВСЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТІ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

У Львівському державному університеті безпеки життєдіяльності є кафедра управління інформаційною безпекою, яка навчає студентів за спеціальністю «Кібербезпека» спеціалізацією «Управління інформаційною безпекою». Випускники можуть навчатися на двох освітніх рівнях - бакалавра та магістра. Основними тематиками навчання є управління безпекою інформаційних систем, організацій і підприємств, розробка та адміністрування інформаційних систем і програмно-апаратних засобів захисту інформації.

Після закінчення навчання випускники можуть працювати фахівцями відділу захисту інформації державних підприємств, банків, приватних компаній та організацій. Також вони можуть працювати як програмісти, системні адміністратори та фахівці із захисту інформації в ІТ-компаніях.

В навчальній програмі бакалавра можна виділити дев’ять блоків навчальних модулів.

Під час навчання студенти вивчають гуманітарні модулі, якими є «Українська мова та культура», «Історія України», «Правознавство та правові основи цивільного захисту», «Соціологія», «Психологія» та «Філософія». Крім того, студенти вивчають іноземну мову кожного семестру.

Наступним блоком є природничо-науковий. Метою даного блоку є надання студентам базових теоретичних знань з математики, фізики та екології, які будуть використовуватися в процесі вивчення інших модулів. Наприклад, в математиці вивчаються такі розділи, як лінійна алгебра та аналітична геометрія, математичний аналіз, теорія ймовірностей, теорія чисел, поля та теорія лишків.

Також наші студенти вивчають економіку та модулі, пов’язані з економічною безпекою та управлінням. Вони знаходяться в блоці «Економічна та організаційна безпека». Основи економіки та управління вивчаються на першому курсі в модулях «Економічна теорія» та «Основи менеджменту». На другому курсі є теорія ризиків, в якій розглядаються поняття ризиків інформаційної безпеки та загроз, методики їх оцінки та класифікація, кількісний та якісний аналіз ризиків.

Наступним модулем цього блоку є «Інформаційне забезпечення управління». Тут розглядаються інформаційні системи як об'єкт управлінської інформаційної діяльності, системи прийняття управлінських рішень, експертні системи.

В модулі «Організація інформаційної безпеки» студенти вивчають стаціонарний і динамічний захист периметра об'єкту, охоронні сигналізації та камери відеоспостереження, проведення зустрічей, конференцій, підписання угод, організацію авторизованого доступу до інформації.

Останнім модулем цього блоку є «Менеджмент інформаційної безпеки», в якому узагальнюється інформація попередніх модулів блоку. Основою цього модуля є міжнародні стандарти інформаційної безпеки ISO 27xxx: ISO 27000 - Системи управління інформаційною безпекою - Огляд і словник, ISO 27001 - Інформаційні технології - Техніка безпеки - Системи управління інформаційною безпекою - Вимоги; ISO 27002 - практика управління інформаційною безпекою - управління інформаційною безпекою, яка може управлятися за допомогою СУІБ (систем управління інформаційною безпекою).

Наступний блок можна назвати «Програмування та інформаційні технології в кібербезпеці». Даний блок починається з модуля «Інформатика», в якому студенти вивчають комп'ютерну апаратуру, системи числення, офісне та інше програмне забезпечення (Word, Excel, Powerpoint), Інтернет (браузери, електронну пошту, пошук інформації), теорію алгоритмів і мову програмування С.

На другому курсі є модуль "Технології програмування", метою якого є вивчення принципів об'єктно-орієнтованого програмування, а також використання мов С ++, С # і Java для розробки програмного забезпечення.

З третього курсу в цьому блоці студенти вивчають модулі, які включають прикладне програмування різних алгоритмів кібербезпеки. У модулі "Комп'ютерні методи в інформаційних процесах і системах" вивчаються розв'язання методів лінійних, нелінійних, диференціальних рівнянь та їх систем, чисельних методів інтегрування та диференціювання, апроксимацію функцій, операції з матрицями тощо. В дисципліні «Теорія інформації» розглядаються основи концепції ймовірнісного підходу до вимірювання обсягу інформації, алгоритми стиснення (коди Шеннона – Фено, Хаффмана, Лемпеля – Зіва, арифметичні), алгоритми корекції помилок (ітераційні, циклічні, коди Хемінга і Боуза – Чаудхурі – Хокквінгема), підготовка сигналів для передачі по каналах зв'язку та їх обробка з використанням перетворення Фур'є.

Протягом останніх трьох семестрів вивчаються модулі, пов'язані з криптографічним та стеганографічним методами захисту інформації - «Алгоритмічні основи криптології», «Прикладна криптологія» і «Основи стеганографії». У цих модулях є такі теми, як математичні основи крипто-

графії, криптографічні протоколи, криптографічні алгоритми з відкритим ключем (RSA, Рабіна, Ель Гамаля, Діффі Хеллмана, рюкзака, Мак Еліса), криптографія еліптичних кривих, симетричні криптосистеми (шифри на основі мережі Фейстеля, AES, потокові шифри A5), стеганографічні алгоритми приховування інформації в просторових і частотних доменах.

Також у цьому блоці студенти вивчають «WEB програмування» (HTML, CSS, JavaScript) і «Бази даних» (MySQL).

В блоці «Технічний захист інформації» викладаються два модуля цього блоку - «Мікропроцесори в системах технічного захисту» і «Основи технічного захисту». У першому з них вивчаються структура мікропроцесорів і мікроконтролерів, а також принципи асемблерного програмування пристроїв захисту інформації, а в другому - спрямовані антени, типи мікрофонів і електромагнітних пристроїв для отримання інформації, електромагнітне випромінювання каналів зв'язку і моніторів, методи екранування і захист від поширення звуку, генератори шуму.

Наступний блок, можливо, найбільше пов'язаний з кібербезпекою і називається "Інформаційна безпека в комп'ютерних системах і мережах". Цей блок починають на третьому курсі модулем "Комп'ютерні мережі". У цьому розглядаються принципи проектування комп'ютерних мереж, типи комп'ютерних мереж (провідні мережні Ethernet і бездротові мережі Bluetooth, WIFI, WIMax, мобільні). У модулях «Операційні системи» і «Стандарти і протоколи інформаційної безпеки» студенти вивчають операційні системи Windows і CentOS (Linux), а також стандарти і протоколи, які використовують під час обміну інформацією з використанням цих операційних систем (IP, TCP, ARP, ICMP, HTTPS, SSH, SSL, WPA).

Підсумковими модулями цього блоку є «Інформаційна безпека в інформаційно-комунікаційних системах» і «Системи банківської безпеки», в яких вивчають сканери портів і вразливостей, аналізатори кодів, проектування захищених WEB-серверів, пакетні аналізатори (сніфери), інструменти Kali Linux, інструментарії цифрової криміналістики, брандмауери та IDS для захисту мережі.

Існує ще один блок базового навчання - «Комплексна інформаційна безпека». У цьому вивчаються модулі, метою яких є створення комплексних систем інформаційної безпеки. Це такі модулі - «Інформаційна безпека держави», «Системи охорони державної таємниці», «Управління спеціальними документами» та «Комплексні системи інформаційної безпеки».

Важливим етапом навчання студентів є практика на підприємствах після 2-го, 3-го і 4-го курсів в IT-компаніях, приватних і державних підприємствах, структурах ДСНС України. Після закінчення навчання студенти виконують дипломні роботи і здають підсумковий іспит.

Після закінчення навчання випускники можуть працювати в багатьох державних і приватних структурах за спеціальностями, пов'язаними із захистом інформації.

УДК 316.422
Литвинчук Н.Ю.
Апарат Ради національної безпеки і оборони України

ФОРМУВАННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Формування та розвиток безпекового середовища у світі сьогодні відбувається під впливом зростання тенденцій до мілітаризації кіберпростору, використання інформаційних технологій для здобуття перемог у конфліктах та війнах. Відбувається поділу сфер впливу у кіберпросторі між світовими центрами сили, зростання їх прагнення порушити на свою користь воєнно-стратегічну рівновагу. Як у 50 роки минулого століття світ вирішував завдання приборкання ядерної енергії, так і сьогодні він постав перед викликом створення режиму використання кіберпростору задля уникнення глобальної катастрофи.

За таких світових тенденцій, а особливо в умовах розпочатої у 2014 році активної фази гібридної агресії Росії проти України для нашої країни стало критично важливим створення національної системи кібербезпеки. З початку 2015 року була розпочата робота над стратегією кібербезпеки.

Вперше до оновленої Стратегії національної безпеки України (Указ Президента України від 26 травня 2015 року № 287) було включено блок положень щодо питань кібербезпеки. Визначені загрози та пріоритетні напрями державної політики з питань національної безпеки щодо забезпечення кібербезпеки і безпеки інформаційних ресурсів.

15 березня 2016 року Президент України своїм Указом № 96 увів в дію рішення РНБО України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Стратегія визначила метою свої реалізації створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. І найголовніше – прийняття цього документу дозволило на системній основі здійснювати формування національної системи кібербезпеки.

Одним із основних завдань у розбудові національної системи стало удосконалення законодавства у сфері забезпечення кібербезпеки.

Визначною подією у цьому сенсі стало прийняття Верховною Радою України у жовтні 2017 року Закону України «Про основні засади забезпечення кібербезпеки України», який набув чинності 9 травня 2018 року. Цей документ у сукупності зі Стратегією та схваленою у грудні 2017 року Кабінетом Міністрів України Концепцією створення державної системи захисту критичної інфраструктури заклав підґрунтя для розвитку системи кіберзахисту об’єктів критичної інфраструктури.

На підставі зазначеного закону Держспецзв'язку спільно з СБУ, іншими державними органами розроблені нормативно-правові акти, які наразі перебувають на розгляді в Кабінеті Міністрів України і стосуються затвердження вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури, формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури»:

Також Міністерством економічного розвитку і торгівлі України розроблено проект Закону України «Про критичну інфраструктуру та її захист». Вказаний законопроект містить безпосередні критерії, за сукупністю яких повинен відбуватися процес віднесення об'єктів до критичної інфраструктури, порядок категоризації та паспортизації таких об'єктів, складання та ведення їх реєстру, а також вирішуватися завдання з кіберзахисту суб'єктів державної системи захисту критичної інфраструктури та загальні вимоги з кіберзахисту до операторів критичної інфраструктури.

Відсутність Переліку об'єктів критичної інфраструктури суттєво ускладнює кіберзахист таких об'єктів, посилює рівень загроз національній безпеці у сфері кібербезпеки. В таких умовах штабом Антитерористичного центру при СБУ скориговано Перелік об'єктів можливих терористичних посягань за категоріями уразливості на території України, до якого включено 1 598 об'єктів, уразливих у терористичному відношенні.

За результатами опрацювання органами СБУ інформації щодо кіберпосягань на об'єкти критично важливої інфраструктури здійснюється відповідне інформування органів влади.

У контексті кіберзахисту об'єктів критичної інфраструктури актуальним є питання функціонування єдиної інтерактивної бази даних про кіберінциденти, створення якої планується завершити до кінця 2018 року.

Варто зазначити, що завдяки розробленому протоколу спільних дій суб'єктів забезпечення кібербезпеки, власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак та кіберінцидентів, та застосуванню розробленого механізму під час кібератак на об'єкти критичної інфраструктури у минулому році вдалося блокувати та локалізувати поширення кіберінцидентів. Наразі розроблений суб'єктами та узагальнений Держспецзв'язку відповідний проект постанови Кабінету Міністрів України готується до подання в установленому порядку на розгляд Уряду.

Принципово важливим для забезпечення національних інтересів країни стало вирішення проблеми технологічної залежності України від Росії щодо програмного забезпечення.

Кіберпростір, який є потужним технологічним арсеналом розвитку нашого суспільства, поряд із цим став середовищем реалізації загроз національній безпеці держави спецслужбами іноземних держав, насамперед

РФ через тотальне використання на об'єктах критичної інфраструктури програмного забезпечення та телекомунікаційного обладнання, розробленого або виготовленого суб'єктами господарювання держави-агресора. У зв'язку із цим низкою рішень РНБО про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій) до російських виробників зазначеної продукції, зокрема в частині надання в Україні телекомунікаційних послуг і використання телекомунікаційних мереж. Рішенням Ради національної безпеки і оборони України від 2 травня 2018 року уведеним в дію Указом Президента України від 14.05.2018 №126 розширено список юридичних та фізичних осіб РФ до яких застосовано економічні та інші обмежувальні заходи (санкції).

Загалом від початку дій санкцій під ними перебуває 1748 фізичних і 756 юридичних осіб,припинено діяльність в українському сегменті мережі Інтернет 192 сайтів.

Також Держспецзв'язку спільно з СБ України розроблений проект постанови КМУ «Про реалізацію і моніторинг виконання спеціальних економічних та інших обмежувальних заходів (санкцій) щодо припинення надання телекомунікаційних послуг».

В рамках реалізації Трастового фонду НАТО зі сприяння Україні в зміцненні її спроможностей у сфері кібербезпеки створено важливу технологічну складову національної системи кібербезпеки – Ситуаційний центр забезпечення кібербезпеки СБ України та Державний центр кіберзахисту та протидії кіберзагрозам Держспецзв'язку.

На виконання рішення РНБО України від 10 липня 2017 року, уведеного в дію Указом Президента України від 30.08.2017 № 254 Кабінет Міністрів України 27 березня ц.р. прийняв рішення про утворення у складі Держспецзв'язку Національного центру оперативно-технічного управління мережами телекомунікацій.

Такі кроки у напрямі створення національної системи кібербезпеки дозволили наростити спроможності суб'єктів забезпечення кібербезпеки щодо кіберзахисту державних інформаційних ресурсів, відбити та мінімізувати наслідки низки потужних кібератак на інформаційно-телекомунікаційні системи державних органів, об'єкти критичної інфраструктури.

Враховуючи активізацію в країні політичних процесів, пов'язаних із проведення наступних виборів Президента України та нового складу Верховної Ради України здійснювалися заходи, спрямовані на посилення спроможностей держави у напрямі протидії деструктивному використанні кіберпростору, несанкціонованому втручанню в роботу інформаційно-телекомунікаційних систем для реалізації загроз національній безпеці, зокрема спецслужбами іноземних держав, насамперед Російською Федерацією, з метою дестабілізації ситуації в Україні.

Оцінюючи діяльність державних органів щодо реалізації Стратегії як таку, що загалом відповідає визначеним пріоритетним напрямам забезпечення кібербезпеки, варто окреслити низку найбільш актуальних завдань, реалізація яких затримується та потребує оптимізації процесу:

затвердження проекту постанови Кабінету Міністрів України«Про затвердження Протоколу спільних дій суб'єктів забезпечення кібербезпеки, власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків» відтерміновується через тривалий процес доопрацювань документу та погоджень;

запровадження механізмів державно-приватного партнерства у сферу кіберзахисту потребує детального відпрацювання моделі такого партнерства над розробкою якої працює Держспецзв'язку. Варто зазначити, що Службою безпеки України вживаються системні заходи щодо підвищення рівня взаємодії з приватним сектором у сфері протидії кіберзагрозам національній безпеці.

потребує удосконалення законотворчий процес забезпечення кібербезпеки, що вимагає аналізу та узагальнення напрацьованих пропозицій, а це **7** законопроектів, які перебувають на розгляді у Верховній Раді України, та можливого об'єднання їх в один законопроект. На виконання рішення Національного координаційного центру кібербезпеки від 17.10.2018 суб'єктами забезпечення кібербезпеки таке завдання опрацьоване та відповідні пропозиції направлені до Верховної Ради України;

затримується процес формування та визначення основних індикаторів (показників) ефективності реалізації Стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик), що передбачає.

УДК 004.946+366.636+364.652.4:330.341.424

Мамченко С.М.
доктор педагогічних наук, професор,
Національна академія Служби безпеки України

СОЦІАЛЬНО-КУЛЬТУРНИЙ ВИМІР КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Поняття безпеки починається із безпеки людини і вже потім розглядається безпека суспільства та держави. Дійсно людина є соціальною і її існування поза межами суспільства неможливе у розумінні наповненості та розвитку. У цьому сенсі у свідомості будь-якої особи існування та розвиток можливий лише серед інших. Даний посил є константою людства.

Тоді виникає закономірне запитання: як змінюється поняття безпеки людини в соціумі за час його історичного розвитку. Не відкидаючи ціліс-

ність буття соціуму та економічної складової розглянемо таке явище як соціальна комунікація та її вплив на суспільство та державу. Місце та роль комунікації у соціумі визначальне для формування суспільства, держави. Чим краще відбувається донесення інформації до окремої особи та від неї до соціальної верхівки тим щільніше формуються державно-соціальні структури. Держава завжди пильно контролювала інформаційні канали спілкування між її громадянами. До виникнення комп'ютерного простору контролювати виконання цієї функції було досить нескладно та не призводило до системних порушень. Наприклад: телебачення у прикордонних територіях дозволяло передавати сигнал, але межі його розповсюдження були дуже обмежені і тому не мали впливу на більшість людей, тобто особистостей.

Із розбудовою комп'ютерного простору та широкого впровадження інформаційних технологій у повсякденне життя особи, особливо соціальних мереж, межі спілкування розширилися безмежно. Єдиним бар'єром спілкування залишається мова. З подальшим розвитком соціального програмного забезпечення та впровадження он-лайн перекладачів і цей бар'єр буде подолано і спілкування особистостей відбуватиметься умовно без меж. Мова піде про світове людство. Тоді дійсно постане питання про місце держави у світовому суспільстві. Усвідомлюючи такі наслідки держави з автократичними (РФ, Китай) традиціями починають вводити контрольований доступ до світової мережі Інтернет. Дані обмеження встановлюються на законодавчому рівні та обмежуються технічно, використовуючи для аргументації проблему боротьби з світовим тероризмом, кіберзлочинністю тощо.

Здається все зрозуміло та тенденції явні, навіть закономірності або закони розвитку. Але ні. Залишається один дуже суттєвий фактор впливу на безмежне Інтернет спілкування. Це культура, національні традиції, регіональні особливості соціуму. Для більшості населення традиції міжнаціонального, міжрелігійного, міжкультурного спілкування не сформовані. Вказані обставини не дозволять пройти формування світової спільноти без негативних наслідків. Враховуючи кількість різнокультурних контактів у соціальних мережах наслідки можуть мати негативні наслідки, піднімаючи на поверхню старі конфлікти із болісними спогадами для сторін учасників. Тобто кожен контактер соціальної мережі має бути відповідним чином підготовленим та дипломатом. Це неможливо виконати у найближчий час. Чи пройде перенесення конфліктів у віртуальний світ, а потім у світ реалій? Наш досвід показує що можливий та реальний. Слід зазначити, що перенесення віртуального конфлікту у реальний світ відбувається швидко і для більшої частини суспільства поза Інтернетом неочікувано.

Відсутність масової культури-Інтернет, яка сформована у контактерів, суттєво впливає на безпеку людини, суспільства і навіть на саму

комп'ютерну безпеку. Мова йде про прості речі. Всі розуміють, що інфекції у реальному світі потрібно лікувати. У цифровому або кіберпросторі даний постулат чомусь не виконується. Наприклад, через рік після вірусної атаки, що вразила комп'ютерні мережі України, тільки третина адміністраторів безпеки проводила захисні заходи протидії. Лише третина підготовлених, фахово навчених спеціалістів виконували профілактичні дії. Запитайте себе: чи побудована на Вашому комп'ютері політика локальної безпеки. І Ви зрозумієте масштабність проблеми. Про подальші рівні ієрархії комп'ютерної безпеки мова навіть не йде.

Формування цифрового суспільства, впровадження Інтернету речей, замовлення (фрахтування) місць туризму та відпочинку тощо призводить до появлення цифрового відбитку особи, його цифрове життя. Тобто у кожної особи з'являється цифрова історія. Вона може бути використана по різному. Всім відома технологія Big Data була використана для керування виборами у США та інших країнах. Комерційні фірми повідомляють про накопичення Ваших уподобань для надання кращих пропозицій. При цьому до останнього часу накопичені дані досить легко передавалися іншим фірмам та не мали достатнього захисту. Наприклад: 87 мільйонів акаунтів Facebook збирала фірма Camdridge Analitica через програму оцінки якостей особистості. Коли інформація стала загальновідомою, то користувачі були здивовані обсягом та змістом зібраної інформації про них: особиста переписка та журнали викликів тощо. Прикладів можна навести багато, але ми не усвідомлюємо, що таким чином нам звужують цифровий світ, направляючи фокус уваги на зовсім або не надто важливі речі для особи. Відбувається сугестивний вплив на особу, суспільство, державу.

Подальший розвиток цифрового суспільства призведе до росту важливості цифрової особистості, яка також має бути захищена, оскільки вона починає жити у тому цифровому або комп'ютерному світі. А що буде коли ця цифрова людина буде замінена на іншу, за описом подібна але інакша? Чи є захист персональних даних кібернетичною безпекою?

Західна філософія вже давно визнала та займалася цією проблемою. Це знайшло відображення у великій кількості художніх фільмів, де піднімалася ця проблема. Отже приходимо до висновку, що основна системна проблема кібернетичної безпеки є особа, навіть особистість з її філософськими, соціальними та культурними основами.

УДК 351.864.1, 351.746.1
Меленті Є.О.
кандидат технічних наук,
Інститут підготовки юридичних кадрів для СБ України
Національного юридичного університету
імені Ярослава Мудрого

ВИКОРИСТАННЯ МОДЕЛІ ЗАГРОЗ ДЛЯ ОЦІНКИ РІВНЯ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Загрозливі зміни безпекового середовища вимагають побудови в України надійної, інтегрованої та гнучкої системи протидиверсійного захисту об'єктів критичної інфраструктури. Складові такої системи повинні не допустити можливість вчинення диверсійно-підривних дій або мінімізувати їх наслідки в політичній, економічній, воєнних сферах та кібернетичному просторі. Характерною рисою «гібридної» війни є те, що противник намагатиметься завдати поразки не тільки підрозділам регулярної армії, але й об'єктам критичної інфраструктури, які знаходяться в глибині території. Для реалізації такого сценарію розвитку подій постійно удосконалюються бойові можливості і способи застосування диверсійно-розвідувальних груп. Постійний розвиток форм та способів диверсійних дій в тилу противника, поліпшення тактико-технічних характеристик високоточної зброї та звичайних військових засобів ураження, загрози в кібернетичному просторі обумовлюють досить високі вимоги до національної системи протидиверсійного захисту об'єктів критичної інфраструктури. Звичайно, сучасні надбання науково-технічного прогресу, швидкий розвиток ІТ-технологій дозволяють противнику широко застосовувати тактику інформаційно-психологічних операцій. Також слід додати, що протягом останніх років кібератак через мережу Інтернет зазнавали інформаційно-телекомунікаційні системи державних інституцій, великих компаній, фінансових установ, політичних партій та засобів масової інформації, інформаційна інфраструктура органів військового управління України.

В таких умовах перед силами безпеки та оборони постає актуальне завдання з підвищення рівня захищеності критичної інфраструктури від терористичних посягань і диверсій в інформаційному просторі. З метою вирішення окресленого кола питань та вироблення дієвого механізму протидії диверсійно-підривній діяльності іноземних спецслужб у березні 2016 року введено в дію Стратегію кібербезпеки України, а у жовтні 2017 року підписано Закон України «Про основні засади забезпечення кібербезпеки України», яким визначено основи протидії підривній діяльності в кібернетичній сфері. Прийняття закону надало можливість створення в Державній службі спеціального зв'язку та захисту інформації Центру реа-

гування на кіберзагрози. Також у 2018 році на базі Служби безпеки України спільно з представникам Північно-Атлантичного альянсу сформовано Ситуаційний центр забезпечення кібербезпеки, головними завданнями якого є запобігання кібератакам, встановлення їхнього походження та формування пропозицій із протидії їм. Як визначено статтею 19 Закону України «Про національну безпеку», Служба безпеки України забезпечує державну безпеку, здійснюючи: протидію розвідувально-підривній діяльності проти України; боротьбу з тероризмом; контрозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, економічної та інформаційної безпеки держави, об'єктів критичної інфраструктури; охорону державної таємниці. Таким чином, протидія розвідувально-підривній діяльності в інформаційній сфері є також однією з важливих задач, які покладаються на Службу безпеки України.

В розрізі становлення й розвитку єдиної національної системи захисту об'єктів критичної інфраструктури неодмінно слід приділити увагу питанням забезпечення інформаційної безпеки та кіберзахисту таких об'єктів, що в свою чергу вимагає вироблення дієвої протидії таким загрозам. Отже, для встановлення пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, необхідно визначити рівень інформаційної захищеності таких об'єктів критичної інфраструктури. Враховуючи набутий позитивний досвід, до цих заходів доцільно залучити представників Служби безпеки України в якості експертів для проведення комплексної оцінки кіберзагроз щодо об'єктів критичної інфраструктури (насампред, кібертероризм та кібердиверсії). Також потребує удосконалення порядок проведення зазначених перевірок та визначення рівня захищеності об'єктів критичної інфраструктури, виявлення уразливих місць в системі безпеки. Зазначену процедуру, повноваження та завдання Служби безпеки України в сфері захисту об'єктів критичної інфраструктури доцільно врахувати в новій редакції Закону України «Про Службу безпеки України».

З метою упорядкування та систематизації можливих загроз та кібератак на об'єкти критичної інфраструктури в доповіді запропоновано використовувати модель загроз для типового об'єкту критичної інфраструктури. Особливістю застосування загальноприйнятого підходу є те, що усі загрози розподіляються за наслідками їх негативного впливу. Використання такої моделі забезпечить подальше всебічне та повне визначення рівня захищеності об'єктів критичної інфраструктури й оцінку уразливості інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Використання моделі загроз дозволить систематизувати можливі інциденти, з'ясувати причини, фактори їх виникнення та виробити ефективні заходи протидії й забезпечення стійкості функціонування об'єктів критичної інфраструктури.

УДК 350
Мельник Д.С.
кандидат юридичних наук,
старший науковий співробітник,
Служба безпеки України

ЩОДО ПРОБЛЕМНИХ АСПЕКТІВ ПРОТИДІЇ ВИКОРИСТАННЮ КРИПТОВАЛЮТ У ПРОТИПРАВНІЙ ДІЯЛЬНОСТІ В УКРАЇНІ

З огляду на участь України у глобальних світових процесах, протягом останніх трьох років в Україні все більшої популярності набуває створення криптовалют та проведення операцій з ними, на високу активність яких ще донедавна впливало стрімке зростання курсу криптовалют.

В сучасних умовах високій популярності криптовалют в Україні сприяють їх невизначений правовий статус та анонімність, децентралізованість створення («майнінгу») та безконтрольність обігу криптовалют, які нівелюють можливості органів фінмоніторингу та сприяють їх активному використанню організаціями, групами і особами як у цілком легальній, так і у протиправній діяльності.

На сьогодні на міжнародному рівні відсутні єдині стандарти регулювання діяльності у сфері створення і обігу криптовалют, їх контролю і моніторингу.

Водночас Директива ЄС 2015/849 по боротьбі з відмиванням грошей передбачає можливість використання криптовалют з цією метою та визначає повноваження підрозділів Фінансової розвідки (FIU) щодо отримання доступу до інформації про криптовалютні гаманці та біржі.

FATF за дорученням лідерів країн G-20 здійснює підготовку єдиних стандартів регулювання діяльності у сфері створення і обігу криптовалют, їх контролю і моніторингу, а також ідентифікації і розслідування пов'язаної з ними протиправної діяльності (оприлюднення заплановане на червень 2019 року).

Наразі лише окремі держави *(Бразилія, Білорусь, Сінгапур, США, Японія)* визначилися у правовому статусі криптовалюти та вжили заходів щодо законодавчого врегулювання їх обігу. Зокрема, Президент Республіки Білорусь у 2017 році видав указ про «майнінг» криптовалют та порядок їх використання, а також розпорядження щодо створення в країні Парку високих технологій. Однак поняття «криптовалюта» та порядок її створення й операцій з нею залишаються неврегульованими нормами законодавства України.

НБУ, НКЦПФР і Нацфінпослуг України у спільній заяві від 30.11.2017 визнали, що складна правова природа криптовалют не дозволяє визнати їх ані грошовими коштами, ані валютою і платіжним засобом ін-

шої країни чи валютною цінністю, ані електронними грошима, ані цінними паперами чи грошовими сурогатами. Разом з тим фінансові регулятори заявили про триваюче опрацювання питання щодо правового статусу криптовалют та законодавчого врегулювання операцій з ними з урахуванням позицій регуляторів інших країн та останніх тенденцій в розвитку цифрових технологій.

Представники ГПУ, НПУ, ДФС, ДПС, СЗР та ВС України на міжвідомчої конференції «Використання криптовалюти у відмиванні коштів та фінансуванні тероризму: питання превенції в Україні» 16.05.2018 визначили потребу розробки загальнодержавної стратегії контролю обігу віртуальної валюти.

На сьогодні у ВР України опрацьовується три законопроекти щодо унормування обігу криптовалют в Україні: № 7183 від 06.10.2017 «Про обіг криптовалюти в Україні»; № 7183-1 від 10.10.2017 «Про стимулювання ринку криптовалют та їх похідних в Україні» та № 7246 від 30.10.2017 «Про внесення змін до Податкового кодексу України (щодо стимулювання ринку криптовалют та їх похідних в Україні)». Однак представники експертного співтовариства критично ставляться до перспектив прийняття вказаних законопроектів у найближчій перспективі та виражають переконання у необхідності розробки та прийняття принципово нового законодавства у цій сфері.

Разом з тим, сучасні світові тенденції свідчать про активне використання криптовалют у протиправній діяльності: для легалізації доходів, одержаних злочинним шляхом, фінансування терористичної й сепаратистської діяльності, посягань на конституційний лад та державну владу, протиправного виведення капіталів за кордон, внаслідок чого виникають численні загрози та ризики для національної безпеки багатьох держав світу, у т.ч. й України.

Зокрема, Міністерство юстиції США заявило про викриті факти використання РФ криптовалюти для фінансування ведення підривної діяльності на американській території, у т.ч. хакерські атаки на державні установи протягом 2014 – 2018 років та втручання у вибори Президента США у 2016 році.

Також у звіті Мін’юсту США про боротьбу з торгівлею наркотиками за 2017 рік зазначено про використання операцій з криптовалютами для оплати поставок наркотиків та відмивання коштів, отриманих злочинним шляхом.

У грудні 2017 року Федеральною прокуратурою США спільно з Об’єднаним АТЦ ФБР (м. Нью-Йорк) було викрито факт використання криптовалюти для відмивання коштів, отриманих злочинним шляхом, та подальшого фінансування терористичної організації ІДІЛ.

Не є винятком і Україна. Так, у лютому п.р. саме розрахунки у криптовалюті офіційно визнано СБУ одним із головних механізмів фінансування т.зв. «ДНР/ЛНР». Попередньо 01.02.2018 прес-центром СБУ офіційно повідомлено про викритий механізм фінансування НЗВФ т.зв. «ДНР/ЛНР» та діяльності антиукраїнських Інтернет-ресурсів з використанням криптовалют.

Також протягом 2016-2018 років невстановленими особами здійснювалося блокування сайтів низки державних установ та ураження їх інформаційних ресурсів шкідливим програмним забезпеченням з вимогами винагороди у криптовалюті за їх розблокування.

Окрім того, за даними вітчизняних ЗМІ, органами ДПС, ДФС та НПУ у 2018 році викрито низку фактів контрабандного ввезення до України партій обладнання для «майнінгу» криптовалют, його незаконного переміщення через лінію розмежування на ТОТ Донецької і Луганської областей та використання у протиправних цілях (у розрахунках за наркотичні засоби).

Викладене свідчить про нагальну необхідність організації спільно з іноземними партнерами ефективної протидії використанню криптовалют у протиправній діяльності як в Україні, так і поза її межами, не очікуючи законодавчого врегулювання їх правового статусу.

УДК 621.391:519.2

Мостюк Д.Л.
ІСЗЗІ КПІ ім. Ігоря Сікорського
Конюшок С.М.
кандидат технічних наук, доцент,
ІСЗЗІ КПІ ім. Ігоря Сікорського

АНАЛІЗ ВЛАСТИВОСТЕЙ БУЛЕВИХ ФУНКЦІЙ, ЯКІ ВИЗНАЧАЮТЬ СТІЙКІСТЬ КРИПТОСИСТЕМ

В Доктрині інформаційної безпеки України [1] визначені національні інтереси України в інформаційній сфері, де серед життєво важливих інтересів суспільства і держави виділені захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом. Завдання щодо забезпечення в межах компетенції формування і реалізації державної політики у сферах організації спеціального зв’язку та захисту інформації в зазначеному нормативно-правовому акті покладаються на Державну службу спеціального зв’язку та захисту інформації України (далі – Держспецзв’язку). Відповідно до визначених завдань, на Держспецзв’язку покладені обов’язки, що визначені в статті 14 Закону України "Про Державну

службу спеціального зв’язку та захисту інформації України" [2], де з 92 пунктів виділимо наступні:

– розробка критеріїв і порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах; організація та проведення оцінки стану захищеності державних інформаційних ресурсів;

– допуск до експлуатації засобів криптографічного захисту службової інформації та інформації, що становить державну таємницю, засобів, комплексів та систем спеціального зв’язку, визначення криптографічних алгоритмів для застосування у засобах криптографічного захисту інформації;

– визначення криптографічних алгоритмів як рекомендованих, допуску до експлуатації засобів криптографічного захисту інформації, засобів, комплексів та систем спеціального зв’язку;

– проведення відповідно до законодавства заходів щодо реалізації науково-технічної політики, організації наукового забезпечення функціонування і розвитку сфер спеціального зв’язку та захисту інформації, телекомунікацій, користування радіочастотним ресурсом України.

Таким чином, актуальною є задача створення та підтримання умов, які гарантують безпечну обробку, зберігання та передачу державних інформаційних ресурсів. Для вирішення цієї задачі, поряд з технічними та організаційними, застосовують криптографічні методи, які базуються на спеціальних математичних перетвореннях інформації, що захищається [3, 4]. На даний час без криптографічних методів та засобів неможливо вирішення таких задач інформаційної безпеки як забезпечення конфіденційності, цілісності, автентичності, невідстежуваності (анонімності), неможливості відмови від авторства тощо. Тому рівень розвитку криптографічних методів, які використовуються для захисту державних інформаційних ресурсів, суттєво впливає на інформаційну безпеку держави в цілому, її економічну незалежність та суверенітет.

Найважливішою вимогою до криптографічних алгоритмів та протоколів є умова їх практичної стійкості відносно всіх відомих криптоаналітичних атак. Якщо ця вимога не виконується, то інші характеристики криптоалгоритму втрачають своє значення. В той же час, отримання науково обґрунтованих оцінок стійкості криптографічних алгоритмів (навіть відносно конкретних, добре вивчених методів криптоаналізу) є складною науковою проблемою. У зв’язку з цим особливу гостроту набуває проблема обґрунтування стійкості криптоалгоритмів, призначених для захисту інформації в спеціальних інформаційно-телекомунікаційних системах України.

Дослідження стійкості сучасних криптографічних алгоритмів та протоколів, часто потребує аналізу відповідних властивостей булевих функцій (що залежать від десятків чи сотен змінних) [5, 6].

В доповіді представленні результати аналізу існуючих властивостей булевих функцій, зокрема: врівноваженість, нелінійність, лавинна характеристика, кореляційна імунність, алгебраїчна імунність, відсутність заборон. Показано, що ці властивості часто суперечать одна одній, що змушує вибирати найважливіші властивості та формувати збалансований компроміс між ними, для побудови стійких криптосистем.

Запропоновані в доповіді результати дозволяють сформувати перелік ключових властивостей за якими можна обирати булеві функцій при конструюванні та оцінці стійкості криптографічних алгоритмів.

Література

1 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України" : Указ Президента України; Доктрина від 25.02.2017 № 47/2017 // База даних "Законодавство України" / ВР України. URL: https://zakon.rada.gov.ua/laws/show/ 47/2017 (дата звернення 07.03.2019).

2. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних "Законодавство України" / ВР України. URL: https://zakon.rada.gov.ua/laws/show/3475-15 (дата звернення 07.03.2019).

3. Задірака В.К. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: Навчальний посібник / В.К. Задірака, А.М. Кудін, В.О. Людвіченко, О.С. Олексюк. Київ – Тернопіль : Підручники і посібники, 2007. – 272 с.

4. Ковальчук Л.В. Теоретична криптологія: основи алгебри та теорії чисел / Л.В. Ковальчук, С.М. Конюшок, Н.В. Кучинська. Київ : ІСЗЗІ НТУУ "КПІ", 2015. – 184 с.

5. Олексійчук А.М. Засоби та комплекси криптографічного захисту інформації. Частина 1. Вступ до теорії булевих функцій та її криптографічних застосувань: навчальний посібник / А.М. Олексійчук, С.М. Конюшок, Р.В. Проскуровський. Київ : ІСЗЗІ НТУУ "КПІ", 2012. – 188 с.

6. Chuan-Kun Wu. Boolean Functions and Their Applications in Cryptography / Chuan-Kun Wu, Dengguo Feng. Springer-Verlag Berlin Heidelberg, 2016. – p. 267.

УДК 004.056.5: 004.414.22

Нікітіна Є.О.
НТУ «Дніпровська політехніка»
Тимофєєв Д.С.
НТУ «Дніпровська політехніка»

ІНСТРУМЕНТИ ПРОАКТИВНОГО АНАЛІЗУ КІБЕРЗАГРОЗ

В процесі аудитів центрів забезпечення безпеки (SOC) виявлено, що одним з найпоширеніших слабких місць є процес Threat Intelligence (TI) та

інтеграція зібраної інформації. Однією з задач TI є підтримка формування планів з придбання та оновлення програмно-апаратних рішень.

Threat Hunting – процес проактивного пошуку та виявлення загроз, які не можна виявити, використовуючи традиційні заходи захисту (IDS, SIEM тощо). Це переважно ручний процес з елементами автоматизації. Задачею аналітика є збір даних з вузлів, мереж, систем контролю та доступу, джерел OSINT (Open Source Intelligence) та застосування до них технік, що дозволяють здійснити візуалізацію, статистичний аналіз тощо. Аналітик повинен мати достатній рівень знань та кваліфікацію.

Threat Intelligence – процес регулярного та системного збору інформації про загрози, застосування цих даних для захисту систем. TI – це не лише бази сигнатур для Intrusion Detection System (IDS) або набори правил для Security Information and Event Management (SIEM). TI – це процеси, які мають власників, цілі, вимоги та результат.

Існує два рівня TI – стратегічний і тактичний (технічний). Вони відрізняються за результатами та способами використання цих результатів.

Розглянемо основні платформи реалізації процесу.

1. Collective Intelligence Framework (CIF). Розроблена REN-ISAC. Дозволяє збирати та об`єднувати інформацію про загрози та використовувати її для ідентифікації інцидентів, виявлення та нейтралізації загроз. Нейтралізація полягає в генерації правил для Snort (безкоштовна система виявлення атак з відкритим результатом), iptables та інших засобів захисту. Працює переважно з IP-адресами, доменними іменами та URL, які пов`язані зі шкідливою активністю. Формат зберігання інформації – IODEF [1].

2. AlienVault Open Threat eXchange (OTX). Побудований на Open Source SIEM. Може обмінюватись даними з CIF. Надає інформацію про спрямування загроз на об`єкти захисту. Дає змогу синхронізувати аналіз загроз, доступний в OTX, з інструментами, які зазвичай використовуються організацією для моніторингу середовища [2].

3. Collaborative Research Into Threats (CRITs) – ресурс, на якому зберігаються шкідливі програми з відкритим кодом. Мета – створення платформи для спільної роботи з даними, що стосуються загроз безпеці інформації [3].

4. ElectricIQ. Дана платформа зв`язана з провідними аналітиками кіберзагроз, джерелами технічних даних та спільнотами, в яких здійснюється обмін інформацією (наприклад, ISAC). Аналітики в центрах забезпечення безпеки, комп`ютерних групах реагування на надзвичайні ситуації (CERT), Fusion-центрах, розвідувальних групах та групах з пошуку загроз мають змогу швидко розпізнавати діючі та релевантні відомості, взаємодіяти з іншими аналітиками, здійснювати оновлення засобів управління безпекою організації та обмінюватись інформацією із зовнішніми спільнотами [4].

5. ThreatQ. В основі лежить підхід, орієнтований на загрозах інформаційної безпеки. Цей підхід дозволяє групам безпеки розставляти пріоритети на основі загроз та ризиків, співпрацювати з іншими групами, автоматизувати дії та робочі процеси [5].

6. CTX/Soltra Edge. Промислове програмне забезпечення, яке автоматизує процеси, котрі дозволяють обмінюватись інформацією про кіберзагрози, отримувати, перевіряти та реагувати на неї [6].

На етапі вибору платформи, що буде використана в процесі TI, слід визначити основні фактори впливу на кінцеве рішення. Серед таких факторів можна виділити системне та прикладне програмне забезпечення SOC, кваліфікацію групи аналітики та моніторингу, сталість процесів управління кібербезпекою, потужність систем обробки та зберігання інформації, архітектуру об`єктів контролю та інші.

В цілому, IT є необхідним процесом сучасного SOC, що допомагає розставити пріоритети та прискорити реагування на інциденти інформаційної безпеки. Відповідно до досліджень споживачів TI різних галузей, проведених SANS, користувачі фіксують позитивні зміни в кількох напрямах забезпечення ІБ після впровадження процесу TI.

Література

1. Csirtg [Електронний ресурс]. – Режим доступу: https://csirtgadgets.com/.

2. The World’s First Truly Open Threat Intelligence Community [Електронний ресурс]. – Режим доступу: https://otx.alienvault.com/.

3. Collaborative Research Into Threats [Електронний ресурс]. – Режим доступу: https://crits.github.io/.

4. ElectricIQ [Електронний ресурс]. – Режим доступу: https://www.eclecticiq.com/.

5. Threat Quotient [Електронний ресурс]. – Режим доступу: https://www.threatq.com/.

6. Soltra Edge [Електронний ресурс]. – Режим доступу: https://www.soltra.com/en/.

7. Snort [Електронний ресурс]. – Режим доступу: https://www.snort.org/

8. Офіційний сайт Інституту SANS [Електронний ресурс]. – Режим доступу: www.sans.org.

УДК: 341.1/8

Ожеван М.А.
доктор філософських наук, професор
заслужений діяч науки і техніки України,
Національний інститут стратегічних досліджень

НАСТУПАЛЬНІ ОПЕРАЦІЇ У КІБЕРПРОСТОРІ ТА ПРОБЛЕМА «ПАРАЛЕЛЬНОГО ІНТЕРНЕТУ»

Останні на часі ініціативи у сфері керування національними фрагментами Інтернету,характерні як для демократичних, так і диктаторських або

авторитарних країн, спрямовані на його автономізацію і є вельми небезпечними, оскільки можуть обернутися фрагментацією глобального інформаційного простору й утворенням на місці Інтернету «Розщепленої Павутини» (Сплінтернету»; англ. «Splinternet») з багатьма «паралельними Інтернетами» [1].

Головною причиною подібних «експериментальних акцій» є передусім перспектива наступальних кібероперацій у Світовій Мережі, про яку досить відверто заявило на рівні керівних державних документів американське керівництво на чолі з Дональдом Трампом і яку підтримало керівництво НАТО, яке має намір створити у 2023 р. натовське Кіберкомандування [2].

Іншою вагомою причиною кібер-фобійта «втечі» в паралельний Інтернет є входження Інтернету у принципову нову фазу розвитку – «Інтернет речей» й пов'язане з цим поширення у всьому світі з 2020 р. мобільної технології 5G, що істотно загострило розщеплення Інтернету по лінії глобального протистояння США – КНР [3]. У цьому контексті дедалі більше західних експертів і політиків висловлюють побоювання, що на місце неоліберального *«Вашингтонського консенсусу»* приходить авторитарний *«Пекінський консенсус»,* який має на увазі Інтернет, контрольований державною владою й відгороджений від зовнішнього світу різними «електронними стінами».

1 червня 2017 р. у КНР набув чинності Закон *«Про кібербезпеку КНР»,* який акцентує на захисті внутрішньої стабільності, декларуючи кінцевою метою «забезпечення мережевого суверенітету країни». Особливу увагу експертів привернула 37-а стаття даного закону, яка зобов'язує «дані, зібрані на території КНР, зберігати тільки в межах Китаю». Закон, проголошує в інтересах суспільної безпеки війну анонімності в Інтернеті й повну ідентифікацію користувачів Мережі.

Серйозне технологічне відставання КНР й РФ від США та їх провідних союзників по НАТО ці країни мають намір долати із використанням економічних війни та промислового шпигунства. З цієї точки зору ці країни зацікавлені у відкритому Інтернеті. З іншого боку, КНР й РФ як країни з авторитарним типом правління дедалі частіше зустрічаються із викликами соціальної напруги, обумовленої тим же технологічним й економічним відставанням, уповільненням економічного зростання тощо, а тому панічно бояться «кольорових революцій» тощо. У цьому розумінні їх більше влаштовує закритий Інтернет.

Саме таку напів-автономну й напів-відкриту модель Інтернету «із російською специфікою» намагається впроваджувати нинішня путінська російська влада, мотивуючи це інтересами національної безпеки, захисту від потенційного американського кібер-удару тощо. До того ж, за умов західних санкцій, накладених на РФ із відомих причин розв'язаної нею гібрид-

ної війни, які дедалі більше посилюються, побоювання російського керівництва щодо західного «блек-ауту», відключення РФ від ключових онлайнових служб і послуг, важко визнати марними. Одну з ініціатив, спрямованих на «привласнення Інтернету»спробували реалізувати російські законотворці. 12 лютого 2019 р., коли Державна Дума РФ проголосувала законопроект №608767-7 *«Про внесення змін у деякі законодавчі акти Російської Федерації (в частині забезпечення безпечного і стійкого функціонування мережі «Інтернет» на території Російської Федерації).* Конкретно йдеться про зміни й доповнення до двох законів – *«Про зв'язок»* і *«Про інформацію, інформаційні технології і захист інформації».*Безпосереднім приводом для прийняття відповідного закону розробники вибрали «безпрецедентно агресивні» американські ініціативи від вересня 2018 р., спрямовані на наступальні кібератаки у відповідь на будь-які напади на кіберпростір самих США. Конкретно йдеться про загрози, пов'язані з насильницьким відключенням «Рунету» від глобальної мережі. Тобто відповідальність за таке відключення покладається на зовнішню сторону (зокрема – на США). У Пояснювальній записці до Проекту федерального закону №608767-7 *«Про внесення змін до деяких законодавчих актів Російської Федерації»* уже в перших абзацах вказано, що він підготовлений «з урахуванням агресивного характеру прийнятої у вересні 2018 року Стратегії національної кібербезпеки США», оскільки у даному документі декларується принцип «збереження миру силою», а Росію безпосередньо і бездоказово звинувачують у скоєнні хакерських атак» і «відверто говориться про [її] покарання», оскільки «ряд безвідповідальних кібератак…завдали шкоди американським і міжнародним компаніям, нашим союзникам і партнерам»…«відповідне покарання…могло б стримувати кібератаки в майбутньому».

У випадку російських інвектив на адресу США йдеться про наступні документи:

– «Національну кіберстратегію США», засновану на основних положеннях ухваленої у грудні 2017 р. Стратегії національної безпеки США.

– Оновлену версію Кіберстратегії Міністерства оборони США – 2018.

– Президентський меморандум з питань національної безпеки 13 (NSPM 13), центральним пунктом якого є питання наступальних кібероперацій, що істотно «розв'язало руки» американським військовим на предмет здійснення подібних операцій, оскільки для цього більше не буде потрібна тривала процедура узгоджень на рівні Білого Дому.

Новий російський Закон спрямований на: (1) створення та впровадження Роскомнадзором національної системи доменних імен, тобто виведення їх з-під контролю відповідної міжнародної служби; (2) мінімізацію поширення поза межі РФ інформації, якою обмінюються користувачі Інтернету всередині Росії, тобто замикання їх комунікацій на російські ко-

реневі сервери; (3) перепорядкування Роскомнадзору Центру моніторингу і управління мережею зв'язку загального користування (досі перебував у складі радіочастотної служби) з метою координації дій операторів зв'язку за умов виникнення загрози; (4) забезпечення можливостей для власників мереж й операторів зв'язку перейти на режим централізованого управління трафіком, його самозамикання на російські кореневі сервери у разі виникнення загрози.

Враховуючи, що Україна також не застрахована у разі виникнення серйозного кібер-конфлікту від загрози часткового відключення від Світової Мережі («блекауту») компетентним українським спецслужбам (найімовірніше – СБУ) за дорученням Президента України доречно розробити реалістичний План дій у ситуації кібервійни проти України з метою автономізації українського сегменту Світової Мережі (Укрнету), пов'язаного з критичною інформаційною інфраструктурою. У даному Плані слід передусім передбачити повний або частковий контроль вхідного та вихідного українського Інтернет-трафику та створення декількох кореневих серверів, на які замикався б у ситуаціях масованих кібернападів на Україну внутрішній Інтернет-трафик. Водночас план повинен забезпечити матеріально-фінансові можливості як власникам мереж, так операторам зв'язку перейти на критичний позаштатний режим централізованого управління трафіком, його самозамикання на українські кореневі сервери.

Література

1. Joseph S. Nye. Internet orSplinternet? // BelferCenterforScienceandInternationalAffairs. Aug. 10, 2016 [Електронний ресурс] – Режим доступу: https://www.belfercenter.org/publication/internet-or-splinternet.

2. NATO cybercommandtobefullyoperationalin 2023. [Електронний ресурс] – Режим доступу: https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9.

3. Chin, Josh. The Internet, DividedBetweenthe U.S. andChina, HasBecome a Battleground; AsChinaandtheWestracefor 5G dominance, twodigitalpowerswithverydifferentapproachestotechnologyarestakingouttheircorners // WallStreetJournal (Online). 2019. Feb 9. [Електронний ресурс] – Режим доступу: https://www.wsj.com/articles/the-internet-divided-between-the-u-s-and-china-has-become-a-battleground-11549688420.

УДК 351
Пальчик М.Л.
кандидат юридичних наук,
Національна академія Служби безпеки України

ДОСВІД США ПЕРЕВІРКИ ГОТОВНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДО КІБЕРАТАК

В умовах обмеженості ресурсів та стабільно високої загрози кібератак зі сторони Російської Федерації, виконання покладених на Службу безпеки України завдань по забезпеченню кібербезпеки держави може бути реалізовано, у тому числі, шляхом активного залучення фахівців приватного сектору. Одним із таких завдань, в яких максимально повно можна використати потенціал приватного сектору, є проведення негласної перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів.

Аналіз існуючого іноземного досвіду свідчить про те, що в окремих державах вже ініційовано та успішно впроваджено практику залучення приватного сектору до пошуку уразливостей кіберзахисту на об'єктах сектору безпеки і оборони.

Так, в США за ініціативи Міністерства оборони, у 2016 році, у межах перевірки стану кібербезпеки, реалізовано проект "Зламай Пентагон" (Hack the Pentagon). Метою проекту було знаходження проблем та уразливостей у системі кіберзахисту оборонного відомства за допомогою добровольців з числа представників приватного сектору, які спеціалізуються на питаннях кібербезпеки. Фахівцями для тестування були обрані громадяни США, які пройшли процедуру реєстрації та щодо яких було здійснено перевірку біографії. У 2016 році участь у проекті взяли більш ніж 1,4 тисячі "хакерів". Для тестування, в межах діючої ініціативи, спеціалістам були відкриті окремі комп'ютерні мережі на визначений період [1].

Програма тривала з 18-го квітня по 12-е травня 2016 року. Вже через 13 хвилин після запуску програми було повідомлено про першу уразливість в системі кібрезахисту. А протягом перших шести годин подано близько 200 звітів про уразливості. За увесь час реалізації проекту спеціалістам вдалось виявити 1189 уразливостей з яких 138 визнано найбільш небезпечними для системи безпеки сайтів Пентагону.

За кожну виявлену та повідомлену уразливість спеціалістам виплачувалась відповідна грошова винагорода, так званий "bug bounty". Індивідуальні виплати за цим проектом складали від 100 дол. до 15 тис. дол. Розмір виплат залежав від типу та небезпечності виявленої уразливості, а також від того чи зміг "хакер" нею скористатися чи ні. Загальна сума виплат

за програмою склала близько 75 тис. дол. за подані в установленому порядку звіти про уразливість [1].

За словами колишнього міністра оборони США Еша Картера, запровадити таку ініціативу змусив той факт, що військові на сьогодні не володіють достатніми знаннями в індустрії інформаційної безпеки, саме тому дії по залученню кращих представників були усвідомленою необхідністю забезпечення кібербезпеки на сучасному етапі. При цьому, за інформацією керівництва оборонного відомства, програма перевершила усі очікування та дозволить у майбутньому зробити інформаційні системи більш безпечними при відносно незначних витратах [2].

Ще однією подібною ініціативою в США є програма "Зламай Військово-повітряні сили". Останню таку програму було реалізовано у період з 19 жовтня по 22 листопада 2018 року За час програми було виявлено та усунено понад 120 уразливостей кібрезахисту військово-повітряних сил США, та здійснено виплати на загальну суму 130 тис. дол. Це була сьома подібна ініціатива за участі оборонного відомства США та третя за участі Військово-повітряних сил США [3].

Як можемо бачити в США вже сформовано позитивну практику залучення фахівців приватного сектору до перевірки готовності об'єктів критичної інфраструктури до кібератак. Подібні ініціативи офіційно санкціонуються на визначений проміжок часу, для визначених категорій осіб, що одночасно виключає несанкціонованість доступу до інформаційних ресурсів, а також дозволяє обмежити доступ до них.

В межах підготовленої публікації нами вивчено лише окремі аспекти існуючих ініціатив державно-приватної взаємодії по забезпеченню кібербезпеки в США. Водночас вважаємо, що використання органами безпеки нашої держави існуючого іноземного досвіду та апробованих підходів по залученню фахівців приватного сектору до перевірки готовності об'єктів критичної інфраструктури до кібератак та кіберінцидентів, значно допоможе у формуванні дієвої системи реагування на виклики та загрози, що виникають у кіберпросторі.

Література

1. Hack the Pentagon [Електронний ресурс]. – Режим доступу: https://www.hackerone.com/resources/hack-the-pentagon.

2. Програма "Зламай Пентагон" успішно завершилась [Електронний ресурс]. – Режим доступу: https://www.fainaidea.com.

3. «Hack the Air Force» bug hunting challenge uncovers 120 flaws in websites and services [Електронний ресурс]. – Режим доступу: https://www.zdnet.com/article/hack-the-air-force-bug-hunting-challenge-uncovers-120-flaws-in-websites-and-services.

УДК 004.7.056.5(477)(045)
Петров В.В.
кандидат політичних наук,
Апарат РНБО України

ЩОДО ПРОВЕДЕННЯ ОГЛЯДУ СТАНУ КІБЕРЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Загроза несвоєчасного проведення огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури створює передумови до порушення процесу стратегічного планування у сфері національної безпеки та кібербезпеки зокрема.

Мова іде про те, що саме за результатами проведення Комплексного огляду сектору безпеки і оборони, складовою якого є огляд у сфері кібербезпеки, формуються та оновлюються Стратегія національної безпеки України та Стратегія кібербезпеки України.

Чинна стратегія національної безпеки України спрямована на реалізацію визначених нею пріоритетів державної політики національної безпеки до 2020 року. Цей термін свідчить про те, що на часі підготовка нових стратегічних документів за усіма напрямами державної політики з питань національної безпеки, зокрема у сфері кібербезпеки. Тобто впродовж 2020 року необхідно розробити проект нової Стратегії кібербезпеки України, який відповідно до статей 1 та 25 ЗУ «Про національну безпеку України» [1] схвалюється РНБО України та затверджується Президентом України.

Комплексний огляду сектору безпеки і оборони, у свою чергу, проводиться за рішенням РНБО України, яке уводиться в дію відповідним Указом Президента України та включає проведення поряд із оглядами усіх складових сектору безпеки і оборони також огляд стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

Законодавством встановлено, що огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, здійснюється Державною службою спеціального зв'язку та захисту інформації України згідно з порядком, встановленим Кабінетом Міністрів України. Науково-методичне забезпечення проведення комплексного огляду сектору безпеки і оборони здійснює Національний інститут стратегічних досліджень.

У цьому контексті викликає занепокоєння той факт, що Урядом досі не визначений порядок проведення комплексного огляду сектору безпеки і оборони у сфері кібербезпеки. Часу на проведення огляду та формування за його результатами нової Стратегії національної безпеки України та відповідно на її основі нової Стратегії кібербезпеки України залишилося критично мало.

Адміністрацією Держспецзв'язку, для забезпечення реалізації Закону України «Про національну безпеку України», було розроблено проект постанови Кабінету Міністрів України «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» (далі - проект Постанови).

Положення проекту Постанови створюють умови для аналізу ефективності та продуктивності застосованих засобів і заходів з кіберзахисту, повноти та достатності матеріально-технічного, фінансового, кадрового та іншого забезпечення діяльності у сфері захисту інформації та, як наслідок - для вдосконалення заходів, спрямованих на розбудову національної системи кібербезпеки.

Прийняття Постанови дозволить врегулювати питання проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, залучивши до цих заходів всіх суб'єктів діяльності у сфері захисту критичної інфраструктури. Крім того, створить передумови для організації та проведення секторальних (галузевих) та відомчих оглядів стану кіберзахисту, що дозволить оцінити реальний стан справ на всіх об'єктах критичної інформаційної інфраструктури життєво важливих галузей економіки країни, сформувати подальші заходи щодо його вдосконалення й посилення спроможностей інфраструктури країни протистояти сучасним викликам і загрозам у кіберпросторі.

Також слід зазначити, що для проведення повноцінної і належної процедури проведення огляду необхідно прийняти низку підзаконних актів, нормами яких передбачено встановлення як загальних вимог з кіберзахисту об'єктів критичної інфраструктури, так і критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури та формування переліку об'єктів критичної інформаційної інфраструктури.

Викладені факти свідчать, що зволікання із затвердженням Порядку проведення огляду у сфері кіберзахисту, як складової сектору безпеки і оборони, створюють чинники реальної загрози зриву процесу стратегічного планування не тільки у сфері кібербезпеки, а і в усій системі національної безпеки, оскільки оновлення Стратегії національної безпеки України здійснюється саме за результатами проведення Комплексного огляду сектору безпеки і оборони.

Така ситуація вимагає вжиття невідкладних заходів координаційного та контрольного характеру, спрямованих на прискорення процесу забезпечення реалізації положень Закону України «Про національну безпеку України» в частині проведення огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

Література

1. Закон України «Про національну безпеку України» // Відомості Верховної Ради (ВВР). – 2018. – № 31. – Ст. 241.

УДК 342.52
Петров С.Г.
кандидат юридичних наук,
Служба безпека України

ДЕРЖАВНІ ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ ЯК ОБ'ЄКТ КІБЕРАТАК

Останніми роками Україна набуває досвіду протидії кіберагресії, переважно ініційованої спецслужбами Росії. Починаючи з 2014 року російська сторона активно застосовує акції кібернетичного впливу із використанням можливостей підконтрольних хакерських угрупувань, які спрямовуються не лише на державні електронні інформаційні ресурси, а й загалом на руйнування української державності. Протидія кібератакам на об'єкти критичної інформаційної інфраструктури України потребують скоординованих зусиль як на національному, так і на міжнародному рівнях, що дасть змогу Україні та її партнерам об'єднатися у захисті загальноєвропейських цінностей і міжнародної безпеки.

Разом з тим, актуалізуються питання розробки і прийняття нормативно-правових актів з метою забезпечення кібербезпеки держави, об'єктів критичної інфраструктури та їх інформаційних систем. Так, Стратегія кібербезпеки України сформувала основні напрями розвитку відповідного законодавства [1]. Закон України «Про основні засади забезпечення кібербезпеки України» [2] визначив організаційні і правові засади функціонування національної системи кібербезпеки. Згідно із цим Законом, СБ України зокрема розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів.

За останні роки є багато прикладів атак на державні електронні інформаційні ресурси України з боку РФ. Так, у травні 2014 р. потужних кібератаки проводились на інформаційні ресурси Центральної виборчої Комісії, які відбулись під час позачергових виборів Президента України та мали на меті модифікацію інформації та блокування роботи комп'ютерних мереж. Наприкінці 2015 року шкідливим програмним забезпеченням BlackEnergy було виведено з ладу комп'ютерні мережі підприємств енергетичної сфери західних та центральних регіонів України, що залишило без електропостачання сотні тисяч споживачів та створило передумови до зростання соціальної напруги в державі.

У грудні 2016 року здійснено комплекс кібератак на державні електронні інформаційні ресурси фінансового і транспортного секторів України, на деякий час було призупинено обслуговування клієнтів державними фінансовими установами та транспортними компаніями.

27 червня 2017 року відбулась потужна кібератака світового масштабу, відома як Petya/NotPetya, на комп'ютерні мережі банківського, енергетичного, транспортного секторів, об'єктів зв'язку та інших важливих об'єктів критичної інфраструктури, епіцентром якої стала України. Також одним з об'єктів посягання стали державні електронні інформаційні ресурси.

Безумовно, як вірно зазначають науковці, «ефективність співробітництва правоохоронних органів України у розслідуванні кіберзлочинів безпосередньо залежить від деталізованого законодавства, яке б відображало положення Конвенції про кіберзлочинність» [3]. Однак, варто відзначити, що Службою безпеки України налагоджено взаємодію з партнерськими спеціальними службами та правоохоронними органами і міжнародними організаціями, що спеціалізуються на кібернетичній безпеці, розслідуванні кіберзлочинів. СБ України отримала технічне обладнання та програмне забезпечення для роботи Ситуаційного центру кібербезпеки СБУ (далі – Центр) у межах виконання першого етапу Угоди про реалізацію Трастового фонду Україна – НАТО з питань кібербезпеки. Центр забезпечує своєчасне виявлення та реагування на кіберінциденти та формує лабораторію з комп'ютерної криміналістики.

У жовтні 2017 року попереджено проведення організованої російськими спецслужбами кібероперації, спрямованої проти державних електронних інформаційних ресурсів, а саме на блокування роботи органів державної влади України, великих державних компаній і підприємств України, реалізацію якої планували здійснити з використанням оновлень поширеного програмного забезпечення. У квітні 2018 року виявлено та локалізовано кібератаку на об'єкти оборонно-промислового комплексу держави, спрямовану на дискредитацію України у частині ненадійності української сторони у співпраці в науковій та інженерній сферах.

Крім того, Центром виявлено та своєчасно зреаговано на кібератаку, спрямовану на державні електронні інформаційні ресурси сектору безпеки та оборони України, насамперед СБ України, Міноборони України, Держприкордонслужби України, а також підрозділи, які залучені до виконання завдань Операції об'єднаних сил, метою якої було отримання віддаленого доступу та викрадення службової інформації. Зазначена кібератака була здійснена хакерським угрупуванням, яке територіально знаходиться в анексованій АР Крим, із застосуванням шкідливого програмного забезпечення відомого як «Armagedon», яке раніше застосовувалося спецслужбами РФ.

У травні 2018 року Службою безпеки України у взаємодії з представниками міжнародних ІТ-компаній та ФБР США попереджено проведення масштабної кібератаки на державні структури та приватні компанії з метою дестабілізації ситуації під час проведення у Києві фіналу Ліги Чемпіонів УЄФА [4].

Література

1. Указ Президента України від 15.03.2016 № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Офіційний вісник України, 2016, № 23, ст. 899.

2. Закон України від 05.10.2017 «Про основні засади забезпечення кібербезпеки України». Відомості Верховної Ради України, 10.11.2017, № 45, ст. 403.

3. Марущак А. І. Проблеми розслідування кіберзлочинів в Україні. Економіка. Фінанси. Право. 2018. № 1. С. 23-27.

4. Офіційний сайт Служби безпеки України. Режим доступу: www.ssu.gov.ua.

УДК 378

Пучков О.О.
кандидат філософських наук, професор,
ІСЗЗІ КПІ ім. Ігоря Сікорського
Конюшок С.М.
кандидат технічних наук, доцент,
ІСЗЗІ КПІ ім. Ігоря Сікорського

ПІДГОТОВКА ФАХІВЦІВ ДЛЯ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ З ПИТАНЬ КІБЕРБЕЗПЕКИ: ДОСВІД ІСЗЗІ КПІ ІМ. ІГОРЯ СІКОРСЬКОГО

Масштабна гібридна агресія проти України підвищила рівень загроз у сфері національної безпеки і оборони держави, які реалізуються в кіберпросторі. В таких умовах особливо важливими є ефективні кроки, що спрямовані як на подолання кіберзагроз сьогодення, так і на вдосконалення національної системи кібербезпеки, яка має бути спроможна реагувати на будь які виклики.

Одним із шляхів забезпечення функціонування національної системи кібербезпеки визначено підготовку фахівців ступенів вищої освіти бакалавр і магістр за державним замовленням в обсязі, необхідному для задоволення потреб держави, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів [1].

Крім того, Стратегія кібербезпеки України [2] відносить розвиток системи підготовки кадрів для потреб органів сектору безпеки і оборони України та розвиток науково-виробничого потенціалу такої системи до головних заходів, що впливають на розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки.

В Доктрині інформаційної безпеки України [3] визначені національні інтереси України в інформаційній сфері, де серед життєво важливих інтересів суспільства і держави виділені захищеність державної таємниці та

іншої інформації, вимоги щодо захисту якої встановлені законом. Завдання щодо забезпечення в межах компетенції формування і реалізації державної політики у сферах організації спеціального зв'язку та захисту інформації в зазначеному нормативно-правовому акті покладаються на Державну службу спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку). Відповідно до визначених завдань, на Держспецзв'язку покладено обов'язок [4] здійснення разом із центральним органом виконавчої влади в галузі освіти і науки науково-методичного управління підготовкою фахівців у сфері криптографічного та технічного захисту інформації, телекомунікацій, радіотехнологій і радіочастотного ресурсу.

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" (далі – ІСЗЗІ КПІ ім. Ігоря Сікорського) є навчально-науковим структурним підрозділом КПІ ім. Ігоря Сікорського зі статусом закладу освіти Держспецзв'язку. Інститут здійснює освітню діяльність з підготовки, перепідготовки та підвищення кваліфікації офіцерського складу з вищою освітою у сфері спеціального зв'язку та захисту інформації (в тому числі і з питань кібербезпеки) для потреб, насамперед, Держспецзв'язку, а також інших центральних органів виконавчої влади, військових формувань і правоохоронних органів, зокрема, Служби безпеки України, Служби зовнішньої розвідки України, Головного управління розвідки Міністерства оборони України та Управління державної охорони України. Крім того, починаючи з 2007 року в Інституті на підставі міжнародних договорів здійснюється підготовка кадрів в інтересах Комітету національної безпеки Республіки Казахстан.

В доповіді досліджується проблема підготовки фахівців з питань кібербезпеки для потреб органів сектору безпеки і оборони України та викладений досвід в цій сфері ІСЗЗІ КПІ ім. Ігоря Сікорського [5], що вже більше десятиріччя забезпечує підготовку висококваліфікованих офіцерських кадрів, які здатні зміцнювати і розбудовувати національну систему кібербезпеки нашої держави та в якому наразі відбувається щоденна робота, яка має на меті врахування досвіду проведення ООС, а також передових методик підготовки відповідних фахівців НАТО та ЄС.

Література

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних "Законодавство України" / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 07.03.2019).

2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" : Указ Президента України; Стратегія від 15.03.2016 № 96/2016 // База даних "Законодавство України" / ВР України. URL: https://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення 07.03.2019).

3. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України" : Указ Президента України; Доктрина від 25.02.2017 № 47/2017 // База даних "Законодавство України" / ВР України. URL: https://zakon.rada.gov.ua/laws/show/47/2017 (дата звернення 07.03.2019).

4. Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних "Законодавство України" / ВР України. URL: https://zakon.rada.gov.ua/laws/show/3475-15 (дата звернення 07.03.2019).

5. Команда ІСЗЗІ КПІ ім. Ігоря Сікорського посіла ІІІ місце на змаганнях ІТ-фахівців NATO TIDE Hackathon 2019. URL: https://iszzi.kpi.ua/команда-ісззі-кпі-ім-ігоря-сікорськог/ (дата звернення 07.03.2019).

УДК 351.86

Сальнікова О.Ф.
доктор наук з державного управління,
старший науковий співробітник
Національний університет оборони України
імені Івана Черняховського

ВИКЛИКИ КІБЕРБЕЗПЕЦІ ПІД ЧАС ПРЕЗИДЕНТСЬКИХ ТА ПАРЛАМЕНТСЬКИХ ВИБОРІВ В УКРАЇНІ

Агресія Російської Федерації, що триває, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України [1].

Протягом президентських та парламентських виборів в Україні основні зусилля Російської Федерації спрямовуватимуться на розхитування суспільства та утворення негативних суспільних настроїв з метою максимального впливу на результати виборів. Зазначені завдання Російська Федерація буде здійснювати як безпосередньо за допомогою проросійських кандидатів у президенти України та підконтрольні їм засоби масової інформації, так і опосередковано, через дискредитацію чинної влади в усіх сферах діяльності держави.

У 2018 році українські спеціалісти з кібербезпеки змогли заблокувати близько 400 кібератак, форми і методи яких постійно змінювались та удосконалювались, а саме: кібернетичні атаки типу “мережна розвідка; “розподілена відмова в обслуговуванні (DDos); розповсюдження шкідливого програмного забезпечення. Переважали технологічно складні кібернетичні атаки (SQL – injection “створення запитів до баз даних, XS-scripting “міжсайтовий скрипт, LFI-attack “включення локальних файлів), спрямовані на несанкціоновану модифікацію механізмів захисту та інформаційних ресурсів, а також перехоплення інформації в інформаційно-телекомунікаційних системах. Більшість кібернетичних атак направлено на створення провокацій інформаційного характеру.

Зазначимо, що найбільш поширеною загрозою у 2019 році визначено фішингові атаки та застосування цілеспрямованих атак, у тому числі за допомогою штучного інтелекту. Крім того продовжаться: атаки на обліко-

ві записи; викрадення персональних даних; добування криптовалюти [2]. Особливої уваги заслуговує інформація, щодо операцій з втручання у проміжні вибори 2016 року у США, здійснених російським агентством інтернет-досліджень (IRA).

Отже, беззаперечним є той факт, що Російська Федерація буде намагатись вплинути через кібернетичний простір на суспільно-політичні процеси в Україні, тому кібербезпека виборів вимагатиме злагодженої та скоординованої роботи багатьох державних інституцій, насамперед Центральної виборчої комісії. Як результат визначено завдання щодо модернізації та оновлення комплексної системи захисту інформації Автоматизованої інформаційно-телекомунікаційної системи "Державний реєстр виборців та Єдиної інформаційно-аналітичної системи "Вибори із застосуванням для захисту інформації, що передається в системах, сучасних засобів криптографічного захисту інформації.

Література

1. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" від 15.03.2016 № 96/2016 [Електронний ресурс]. – Режим доступу: https://zakon5.rada.gov.ua/laws/show/96/2016.

2. Mapping the Future: Dealing With Pervasive and Persistent Threats [Електронний ресурс]. – Режим доступу: https://www.trendmicro.com/ vinfo/us/security/research-and-analysis/predictions/2019.

УДК 378(477)(094)

Сафонов Ю.М.
доктор економічних наук, професор,
заступник директора з наукової роботи
Дашковська О.В.,
кандидат хімічних наук, доцент,
старший науковий співробітник
Погребняк В.П.,
кандидат технічних наук, професор,
старший науковий співробітник,
ДНУ «Інститут модернізації змісту освіти»

КІБЕРПРОСВІТА – ОСНОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Проблема захисту інформації виникла одночасно з необхідністю обміну нею. Особливої ваги ця проблема набула з виникненням і розвитком глобальних інтернет-мереж, здійснення через них обміну інформацією, починаючи від персональних даних особи і до системного управління різними сферами суспільної діяльності, «електронного» урядування тощо.

В Україні тільки у 2017 році [1] було зареєстровано більше 2,5 тисяч кримінальних правопорушень у сфері кібербезпеки, що у три рази більше, ніж у 2016 році. У зв'язку з цим,попит на спеціалістів з кібербезпеки зростає втричі швидше, ніж на ІТ-спеціалістів у цілому. Гострішою постає проблема кіберпросвіти: оволодіння громадянами компетентностями у сфері кібербезпеки, засобів протидії кіберзлочинам та забезпечення персональної безпеки при спілкуванні в соціальних мережах.

Підготовка фахівців у ЗВО, сфері захисту інформації була розпочата в Україні, коли Постановою КМУ від 13 грудня 2006 року № 1719 була затверджена галузь знань 1701 Інформаційна безпека і бакалаврські напрями підготовки «Безпека інформаційних і комунікаційних систем», «Системи технічного захисту інформації», «Управління інформаційною безпекою». У 2010 році Постановою КМУ від 27 серпня 2010 року № 787 [2] в межах зазначеної галузі знань і бакалаврських напрямів були введені спеціальності «Безпека інформаційних і комунікаційних систем», «Безпека державних інформаційних ресурсів», «Системи технічного захисту інформації», «Управління інформаційною безпекою», «Адміністративний менеджмент у сфері захисту інформації»; в галузі знань 0403 «Системні науки та кібернетика» - спеціальність «Криптологія» для освітньо-кваліфікаційних рівнів спеціаліста, магістра. За цей час НМК з Інформаційної безпеки були розроблені і введені в дію всі галузеві стандарти, біля 40 закладів вищої освіти розпочали підготовку кваліфікованих кадрів із зазначених вище спеціальностей.

У 2015 році Постановою Уряду №266 [3] введена «інтегрована» спеціальність 125 «Кібербезпека» в галузі знань 12 «Інформаційні технології» замість названих вище 5 спеціальностей.

У 2018 році в системі кіберосвіти зроблені наступні кроки:

- успішно завершена розробка СВО зі спеціальності 125 Кібербезпека. Науково-методичною комісією у тісній співпраці з ЗВО, які здійснюють підготовку здобувачів вищої освіти з цієї спеціальності, компаніями-роботодавцями, Держспецзв'язком, Міністерством освіти і науки України, Інститутом модернізації змісту освіти затверджено стандарт вищої освіти бакалавра;

- розпочато розроблення СВО магістра, у зв'язку з чим є можливість організувати підготовку на освітньому рівні магістра за спеціалізаціями:«Безпека інформаційних і комунікаційних систем», «Безпека державних інформаційних ресурсів», «Системи технічного захисту інформації», «Управління інформаційною безпекою», «Адміністративний менеджмент у сфері захисту інформації»; «Криптологія»;

- планується відкриття підготовки фахівців за кваліфікаціями «Майстер з кібербезпеки» та «Молодший бакалавр з кібербезпеки» в закладах професійної освіти та коледжах.

Слід наголосити, що у зв'язку із закінченням повноважень сформованих у 2016 році Сектора вищої освіти Науково-методичної ради Міністерством освіти і науки України та Науково-методичних комісій, нині формуються нові комісії, які будуть розробляти СВО в 2019 році. У ЗВО, ІТ-фірм є можливість рекомендувати своїх представників до їх складу.

Особливої ваги набула проблема забезпечення персональної кіберграмотності населення, особливо молоді: учнівської, студентської як найбільш активних користувачів Інтернет-мереж. За останні роки кількість користувачів соціальних мереж постійно зростає,бо вони доступні кожному, хто має комп'ютер чи сучасний мобільний телефон, забезпечують практично необмежений доступ до величезних масивів різноманітної інформації та можливість спілкування. У той же час, Інтернет став простором, у якому скоюються кіберзлочини, та їх інструментом. Причинами постійного зростання кількості кіберзлочинів, а це поширення комп'ютерних вірусів, шахрайство, викрадення персональної та комерційної інформації, порушення роботи комп'ютерних мереж тощо, є анонімність, доступність інформації, легке збагачення та можливості комп'ютерної техніки, з допомогою якої скоїти злочин можна з любої точки і в любій точці світу [4].

Найслабшою ланкою існуючих кібератак є людський фактор,тому просвітницька діяльність у цьому напрямку є дуже важливою. Викладачі та студенти закладів вищої освіти, вчителі та учні, які є користувачами мережі та освітніх сайтів, можуть постраждати від кіберзлочинців, через них можуть здійснюватися крадіжки інформації, поширення мережевих вірусів тощо. Враховуючи означене, концептуально завдання кіберпросвіти полягає у наступному: оволодіння громадянами компетентностями у сфері кібербезпеки, засобами протидії кіберзлочинам та забезпечення персональної безпеки при спілкуванні в соціальних мережах. На жаль, майже не приділяється уваги темі кібербезпеки в закладах загальної середньої освіти, не вистачає викладачів-фахівцівіз цього питання у коледжах і у закладах ПТО.

Пропонується створити систему розв'язання проблем кіберпросвіти через:

- навчання основам кібербезпеки здобувачів освіти у закладах загальної середньої, професійно-технічної та вищої освіти, ввівши обов'язкові компетентності в державні стандарти ЗСО, ПТО, стандарти вищої освіти та відповідні навчальні дисципліни за вибором закладу в освітні програми і навчальні плани;

- підвищення кваліфікації викладачів та адміністрації закладів освіти в спеціально створених центрах на базі університетів і академій, які готують фахівців з кібербезпеки та у сфері ІТ, в центрах академій Cisco тощо;

- забезпечення надійності комп'ютерних мереж в закладах освіти.

Для досягнення успішного результату необхідна ефективна і скоординована діяльність всіх зацікавлених сторін:закладів освіти,організацій ІТ-сфери, центральних органів виконавчої влади (Міністерство освіти і науки України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України), громадських ІТ-спільнот, міжнародних програм.

З метою покращення захисту співробітників ЗВО та студентів позитивну роль може відіграти створений при Міністерстві освіти і науки України Експертно-консультативний комітет з цифрових технологій в освіті. Він буде дорадчим консультативним органом, що утворений з метою врахування експертної думки та проведення консультацій у процесі підготовки і організації виконання рішень Міністерства в сфері ІТ, сприяння ефективному приватно-державному партнерству в галузі інформаційно-комунікаційних технологій в освіті, підтримання постійного ефективного діалогу із представниками ІТ бізнесу, експертами та громадськими організаціями у сфері ІТ-світу [5].

В Україні є успішні приклади співпраці між закладами вищої освіти, організаціями ІТ-сфери та міжнародними програмами.

У Тернопільському національному технічному університеті імені Івана Пулюя створено Центр підготовки інструкторів з кібербезпеки. Програма навчання складається із курсів академій Cisco, які вже використовують в школах, коледжах, університетах. Це безкоштовні курси «Вступ до кібербезпеки» для ЗЗСО, «Основи кібербезпеки» для коледжів, ЗВО та спеціалізованих закладів, CCNA CyberOperations та CCNA Security для ЗВО.

Фізико-технічний інститут НТУУ «КПІ імені Ігоря Сікорського» отримав можливість безпечного і пільгового Інтернет-доступу до освітніх комп'ютерних мереж, безкоштовного покриття університету «зонтиком безпеки».На жаль, про ці та інші можливості безкоштовного навчання та підвищення кваліфікації педагогічних і науково-педагогічних кадрів мало відомо в освітньому середовищі, недостатньою є популяризація їх можливостей.

ДНУ «Інститут модернізації змісту освіти»організує і здійснює інформаційну підтримку масових заходів, які позитивно впливають на підвищення рівня освіти і науки в сфері кібербезпеки, сприяють ознайомленню студентської молоді правилам безпечної поведінки в інформаційному просторі [6, 7]. Це Всеукраїнські студентські змагання з проблем кібербезпеки, започатковані КНУ імені Тараса Шевченка, щорічна Всеукраїнська студентська олімпіада за спеціальністю «Кібербезпека», регулярні міжнародні та всеукраїнські науково-практичні і науково-методичні конференції викладачів ЗВО, науковців, представників ІТ-фірм, що проводяться уні-

верситетами за участі і підтримки відповідних галузевих органів, регіональних органів виконавчої влади та місцевого самоврядування.

Безумовно, позитивну і визначну роль у розгортанні системної, широкомасштабної кампанії з захисту громадян України від кіберзлочинності могли б відіграти проведені за ініціативи МОН, СБУ,ДССЗЗІ та професійної спільноти спеціальні Парламентські слухання, розроблення і прийняття Концепції з впровадження навчання та інформування населення України з питань кіберзахисту.

Література

1.Сафонов Ю.М., Дашковська О.В., Погребняк В.П. «Підготовка фахівців у сфері кібербезпеки - пріоритети держави». Матеріали IX Науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави». – Київ (НА СБУ), 2018**,** с. 147-150 *(електронна версія)*. 408 с. – http://academy.ssu.gov.ua/ua/page_sci/.

2. Постанова КМУ від 27 серпня 2010 року № 787 «Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра».

3. Постанова КМУ від 29.04.2015 р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти». [Електроннийресурс]. − Режим доступу:http://tntu.edu.ua/nv/files/266.pdf.

4. Бондаренко О.С., Рєпін Д.А. «Кіберзлочинність в Україні: причини, ознаки та заходи протидії. [Електроннийресурс]. − Режим доступу:http://www.pap.in.ua/1/2018.

5. Лист ДНУ «ІМЗО» від 25.02.2019 № 22.1/10-620 «Щодо дорадчого консультативного органу з цифрових технологій в освіті». [Електроннийресурс]. − Режим доступу:https://imzo.gov.ua.

6. Лист ДНУ «ІМЗО» від 16.01.2019 № 22.1/10-123 «Про Перелік наукових конференцій з проблем вищої освіти і науки у 2019 році». [Електроннийресурс]. − Режим доступу:https://imzo.gov.ua.

7. Лист ДНУ «ІМЗО» від 08.02.2019 № 22.1/10-405 «Про Перелік міжнародних, всеукраїнських науково-практичних конференцій здобувачів вищої освіти і молодих вчених». [Електроннийресурс]. − Режим доступу:https://imzo.gov.ua.

УДК 342.951:351.9

Ткачук Н.А.
кандидат юридичних наук,
Служба безпеки України

СТРАТЕГІЧНЕ ПЛАНУВАННЯ ТА КОНТРОЛЬ У СФЕРІ КІБЕРБЕЗПЕКИ УКРАЇНИ

Стратегія кібербезпеки України (далі – Стратегія) є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України та концептуальні підходи до формування та реалізації

державної політики у сфері кібербезпеки. Цей документ є базисом стратегічного планування держави у зазначеній галузі, основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України.

За своєю суттю стратегічне планування є адаптивним процесом у рамках якого повинні здійснюватись регулярні розроблення й корекція системи планів, перегляд змісту заходів щодо їх виконання на основі безперервного контролю й оцінки змін, які відбуваються ззовні та всередині системи [1; 55].

Контроль за виконанням стратегій, досягненням цільових орієнтирів, а також їх коригування сучасна теорія державного управління визначає як невід'ємний елемент стратегічного управління. Роль контролю як функції управління полягає в тому, що він є засобом здійснення зворотного зв'язку в системі управління. Головний його сенс полягає у створенні гарантій виконання планових рішень [2; 290].

Разом із тим, в Україні система стратегічного контролю, який би забезпечував об'єктивну оцінку та здійснення корегуючого впливу щодо стану реалізації Стратегії кібербезпеки, а також гарантував виконання її положень, на сьогодні, відсутня.

Наразі, реалізація положень Стратегії відбувається в рамках виконання щорічних планів, які формуються Держспецзв'язку та затверджуються відповідними розпорядженнями Кабінету Міністрів України. Водночас, аналіз стану виконання планів реалізації Стратегії кібербезпеки України на 2016-2018 роки [3-5] свідчить, що вказані документи носять переважно декларативний характер. Так, більшість заходів, передбачених ними, наразі, не виконано або виконано частково чи із простроченням встановлених термінів.

Зокрема, ще й досі залишаються не вирішеними наступні питання: не створено перелік ІТС об'єктів критичної інфраструктури, не імплементовано Конвенцію ЄС про кіберзлочинність, не побудовано захищений датацентр для органів державної влади, не вжито ефективних заходів щодо стимулювання розроблення вітчизняного програмного забезпечення, не імплементовано директиви та стандарти ЄС щодо захисту об'єктів критичної інфраструктури, відсутня система аудиту інформаційної безпеки таких об'єктів, не сформовано основні індикатори стану кібербезпеки, не створено єдину систему виявлення кіберзагроз та платформу обміну інформацією між суб'єктами кібербезпеки тощо.

Хоча всі пункти планів, якими були передбачені ці завдання, містили конкретні кінцеві дати виконання та відповідальних за їх виконання державних суб'єктів. Наприклад, відповідальним органом за виконання 15-ти пунктів із наявних 18-ти, передбачених Планом реалізації Стратегії кібер-

безпеки України на 2018 рік, є Державна служба спеціального зв'язку та захисту інформації України [5].

Крім того, своєчасне та ефективне виконання заходів з реалізації Стратегії значно ускладнює той факт, що плани її реалізації формуються Держспецзв'язку, і відповідно, затверджуються Урядом із порушенням встановленого терміну, а саме – до початку планового року.

Так, план реалізації Стратегії на 2017 рік було затверджено КМУ у березні 2017 року (із простроченням терміну на 3 місяці), а на 2018 рік – у липні 2018 року (із простроченням терміну на 7 місяців). Станом на початок березня 2019 року план реалізації Стратегії на 2019 рік також відсутній. Така ситуація апріорі унеможливлює своєчасне та якісне виконання окремих планових позицій відповідальними державними органами.

Суб'єктами, на які покладені завдання із здійснення контролю щодо цього питання, є Секретар РНБО України (у частині забезпечення контролю за виконанням указу Президента України, яким затверджена Стратегія кібербезпеки) та Кабінет Міністрів України (у частині забезпечення контролю за виконанням розпоряджень КМУ, якими затверджуються щорічні плани реалізації Стратегії). Крім того, питання стану реалізації Стратегії кібербезпеки України раз на рік розглядається на засіданнях Національного координаційного центру кібербезпеки.

Разом з тим, основні завдання стратегічного контролю із надання об'єктивної оцінки та вжиття заходів впливу у випадках неналежної реалізації Стратегії відповідальними суб'єктами, на сьогодні, не здійснюються, а невиконані планові позиції просто переносяться на наступний рік (про що свідчить аналіз текстів планів реалізації Стратегії на 2016-2018 рр.).

Крім того, не створені умови, які б забезпечили можливість здійснення ефективного громадського контролю за станом реалізації Стратегії кібербезпеки, наявність якого, як невід'ємного елементу демократичного цивільного контролю, є одним із основних принципів формування державної політики у всіх сферах національної безпеки. Здійснення такого контролю у сфері кібербезпеки ускладнює відсутність офіційної публічної інформації з боку компетентних державних органів щодо вжитих заходів та стану реалізації Стратегії кібербезпеки України.

Отже, для того, щоб стратегічне планування у сфері кібербезпеки мало не лише декларативний характер, а дійсно було основою подальшої реалізації конкретних заходів, спрямованих на посилення кібербезпекового потенціалу нашої держави, необхідно запровадити дієвий механізм контролю щодо своєчасного та належного виконання документів стратегічного планування всіма без виключення суб'єктами забезпечення кібербезпеки України. А у разі не виконання – повинен працювати механізм адекватного реагування та вжиття відповідних заходів правового впливу та притягнення до відповідальності, у т.ч. дисциплінарного характеру.

Крім того, з метою забезпечення ефективного громадського контролю у сфері кібербезпеки є доцільним передбачити обов'язкове оприлюднення на офіційному сайті Держспецзв'язку (з урахуванням вимог Закону України «Про державну таємницю») узагальнених звітних матеріалів щодо вжитих заходів та стану виконання планів реалізації Стратегії кібербезпеки основними суб'єктами національної системи кібербезпеки України.

Література

1. Гнатенко А. І. Стратегічне планування у сфері державного управління: концептуальні підходи / А.І. Гнатенко // Державне управління та місцеве самоврядування: зб. наук. пр. – Дніпропетровськ: Вид-во ДРІ НАДУ, 2013. – № 3(18). –С. 51-60.

2. Тарасюк Г.М. Контроль в системі управління плановою діяльністю підприємства / Г.М. Тарасюк // Міжнародний збірник наукових праць. – № 1(16). – 2010. – С. 284-299.

3. Розпорядження Кабінету Міністрів України від 24 червня 2016 р. № 140-р «Про затвердження Плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України» [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/440-2016-%D1%80.

4. Розпорядження Кабінету Міністрів України від 10 березня 2017 р. № 155-р «Про затвердження Плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України» [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/155-2017-%D1%80.

5. Розпорядження Кабінету Міністрів України від 11 липня 2018 р. № 481-р «Про затвердження Плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України» [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/481-2018-%D1%80.

УДК 004.056.5 + 004.85

Шевченко А.С.
кандидат технічних наук
Толстих В.А.
Столяр В.В.
Військовий інститут телекомунікацій
та інформатизації імені Героїв Крут

ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ІНЦИДЕНТІВ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Сучасні інциденти порушення кібернетичної безпеки представляють собою ланцюг складних процесів, що досить ускладнює, а інколи й унеможливлює, процедури виявлення кіберзагроз. На сьогоднішній день до інцидентів кібернетичної безпеки (ІКБ) в кібернетичному просторі можна віднести кібернетичні атаки та загрози несанкціонованого доступу.

Для забезпечення виявлення ІКБ в засобах захисту інформації та забезпечення кібернетичної безпеки застосовуються статистичні та сигнатурні методи, методи на основі виявлення аномалій. Використання формальних та сигнатурних методів не дозволяють ефективно запобігти сучасним кібернетичним загрозам. Сповільнене реагування на нові кібернетичні загрози призводить до значних втрат, блокування систем та компрометації великих обсягів конфіденційних даних.

Серед методів захисту інформації, на сьогоднішній день, найбільш перспективними є методи виявлення аномалій. На відміну від статистичних та сигнатурних методів методи виявлення аномалій дозволяють виявляти нові атаки, що дозволяє більш ефективно протистояти сучасним кіберзагрозам.

Для реалізації методів виявлення аномалій в якості математичних апаратів останні роки більш широко впроваджуються в кібербезпеку технології штучного інтелекту, підмножиною яких я методи машинного навчання (МН). Для вирішення завдань забезпечення захисту інформації та кібербезпеки методи МН використовуються в задачах виявлення, класифікації та прогнозування ІКБ.

Результати аналізу останніх публікацій дозволили виділити наступні математичні апарати МН, які використовуються в кібербезпеці: мережі Баєса, штучні нейронні мережі, приховані марковські моделі, метод опорних векторів, фільтри Калмана, методи “випадкового лісу”, методи на основі класифікації асоціативних правил, дерева рішень, кластеризація методом k-середніх, нечітка логіка, метод k-найближчих сусідів та інші.

Значна кількість даних методів не є новими математичними апаратами для вирішення технічних задач і розвиваються протягом не одного десятиліття. Нові сфери застосування та технології дозволили застосувати вказані математичні апарати у галузі кібербезпеки.

На сьогоднішній час до основних засобів, які використовують методи МН відносяться: системи антивірусного захисту, системи виявлення та запобігання вторгненням (IDS/IPS), системи попередження втрати даних (DLP), системи управління інформаційною безпекою та подіями (SIEM), анти-DDOS системи, системи розслідування порушень кібернетичної безпеки та інші системи. Основною їх особливістю є те, що в даних системах МН застосовуються в задачах інтелектуального пошуку ІКБ.

Сучасні методи виявлення, які ґрунтуються на основі розпізнавання сигнатур, відповідності асоціативним правилам, не дозволяють виявляти нові загрози даних про які немає в даних базі загроз. Основним недоліком методів евристичного аналізу є значна кількість хибних спрацювань та пропуску загроз. Використання методів МН в засобах захисту інформації та кібербезпеки дозволить вирішити завдання інтелектуального виявлення кібернетичних загроз, більш ефективно здійснювати класифікацію кіберзагроз, виявляти атаки нульового дня.

ПОГЛЯД НА ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ МОЛОДИХ ВЧЕНИХ І СТУДЕНТІВ

УДК 351

Андрейчук В.С.
Національна академія державного управління
при Президентові України

ПРОГНОЗУВАННЯ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека (ІБ), як складова національної безпеки (НБ), потребує використання всього комплексу механізмів моніторингу та прогнозування, але має свою специфіку. По-перше, ІБ є одним із найбільш технологічних секторів безпеки, що активно використовує сучасні інформаційні технології (ІТ). По-друге, ІБ розглядається як мінімум у двох аспектах: технічному (кібербезпека і кібервійни, тощо) і ідеологічному (пропаганда і інформаційні війни, тощо). По-третє, дані моніторингу, висновки та рекомендації, що надає ІБ, є основою прогнозування у всій галузі національної безпеки. Ми розглянемо особливості напрямків прогнозування в сфері інформаційної безпеки (ПІБ) в контексті її як складової НБ та розвитку сучасних ІТ.

Виділимо три основні напрямки ПІБ: організаційний, технічний, ідеологічний.

До організаційного напрямку ПІБ можемо віднести:

1.1. Прогнозування в сфері інформаційної безпеки як складової національної безпеки.

1.2. Прогнозування у інших складових національної безпеки.

1.3. Прогнозування законодавчо-організаційних заходів і стандартів.

1.4. Прогнозування державно-приватного партнерства.

1.5. Інститути прогнозування в сфері ІБ та НБ [1].

1.6. Прогнозування фінансів та ресурсів для інформаційної безпеки всіх рівнів.

1.7. Прогнозування особливостей ІБ у різних галузях економіки та бізнесу (економіка, медицина, фінанси).

1.8. Прогнозування конференцій, семінарів та інших комунікативних заходів.

1.9. Прогнозування методів HR, KPI, мотивації та стимулювання.

1.10. Прогнозування потреб у підготовці та перепідготовці спеціалістів.

1.11. Прогнозування еміграції, створення бізнес-центрів, розширення представництв вендорів та аутсорсінту.

До технічного напрямку ПІБ можемо віднести:

2.1. Прогнозування архітектури глобальних мереж та технологій зв'язку.

2.2. Прогнозування серверів та локальних мереж.

2.3. Прогнозування датацетрів.

3.4. Прогнозування апаратної платформи та процесорів.

2.5. Прогнозування операційних систем та програмного забезпечення.

2.6. Прогнозування хакерських механізмів та засобів захисту.

2.7. Прогнозування атак і рівня захищеності об'єктів критичної інфраструктури.

2.8. Прогнозування загроз від нових (сучасних) технологій.

2.9. Прогнозування технологій захисту інформації та конкурентної розвідки.

До ідеологічного напрямку ПІБ можемо віднести:

3.1. Прогнозування інформаційної політики та протидії пропаганді

3.2. Прогнозування тенденцій ІБ в інтернеті, соціальних мережах та мобільних комунікаціях.

3.3. Прогнозування конверсії та збільшення продажу через інтернет-канали.

3.4. Прогнозування методів соціальної інженерії.

3.5. Прогнозування в умовах інформаційної та гібридної війни. Стратегічні комунікації.

Запропонований класифікатор не є остаточний, але може бути основою для подальшого діалогу та структуризації системи прогнозування в галузі інформаційної безпеки зокрема, і національної безпеки взагалі.

Далі, розглянемо ПІБ в контексті стрімкого розвитку сучасних інформаційних технологій. Традиційні методи прогнозування за допомогою інформаційних технологій знайшли широке практичне застосування у сучасному житті. Методи математичної статистики. Теорії числових рядів, регресії тощо. Служать основою алгоритмів у відомих програмах обробки даних і прогнозування: починаючи від широковідомого EXCELдо спеціалізованих програм типу SPSS, Statistica тощо. Огляд програмного забезпечення для прогнозування можна знайти в наступній роботі [2]. Спеціальні програми використовуються для обробки даних моніторингу суспільної думки та прогнозування результатів виборів.

Останнім часом, у зв`язку з експоненційним ростом потужностей комп`ютерів, розвитку алгоритмів та програмного забезпечення, стали впроваджуватись у різні аспекти бізнесу та безпеки такі сучасні IT: Big-Data (великі дані), ArtificialIntelligence (Штучний інтелект), MachineLearning (машинне навчання), VirtualandAugmentedReality (віртуальна та доповнена реальність), блокчейн, робототехніка, тощо. Це потребує розробки нових алгоритмів, значного збільшення людського і фінансового ресурсу,

а головне – зміни пріоритетів у системі забезпечення національної безпеки до високотехнологічних секторів та проривних напрямків.

Таким чином, органічне поєднання запропонованого класифікатора прогнозування у сфері інформаційної безпеки і сучасних інформаційних технологій прогнозування радикально покращить рівень інформаційної безпеки як складової національної безпеки.

Література

1. Андрейчук В. С. Інституційні аспекти ІТ прогнозування в системі національної безпеки України / В. С. Андрейчук // Вісн. НАДУ, Серія "Державне управління". – 2018. – № 3. – С. 171-180.

2. Ulrich Kuesters , B.D. McCullough , Michael Bell . Forecasting software: Past, present and future// International Journal of Forecasting. – No. 22. – 2006. – P. 599-615.

УДК 351:74

Безкровна Д.О.
Національна академія Служби безпеки України

ДЕЯКІ АСПЕКТИ УДОСКОНАЛЕННЯ ПРАВОВОЇ РЕГЛАМЕНТАЦІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Останнім часом спостерігається загальносвітова тенденція зростання рівня кіберзлочинності. На жаль, сьогодні наша держава поряд із Бразилією, Китаєм, Індією та іншими країнами стає міжнародним центром зазначеної протиправної діяльності [1]. Так, розкрадання коштів в системах інтернет-банкінгу, даних кредитних карт, шахрайство в інформаційних мережах та інсайдерські витоки інформації стають повсякденними явищами на вітчизняних теренах [1]. Тому, задля удосконалення вітчизняного законодавства у сфері забезпечення інформаційної безпеки, зокрема, боротьби із кіберзлочинністю, слід розглянути досвід провідних держав у вказаній сфері.

На сьогоднішній день у багатьох зарубіжних країнах налагоджена система співробітництва та обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки, зокрема США та більшість країн ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинності на ключові позиції [2]. У ряді міждержавних нормативно-правових актів визнано, що кіберзлочинність сьогодні становить загрозу не тільки національній безпеці окремої держави, а й загрожує людству в цілому. Саме тому цій проблемі приділяється значна увага у багатьох державах [3, 4, 5].

Для України така тенденція є, в цілому, позитивною, так, надзвичайно цінною є можливість ознайомлення з досвідом провідних держав світу, які працюють в зазначеному напрямку не перший рік. І хоча загальний вигляд

такої стратегії може сильно варіюватися залежно від політики та об'єктивних і суб'єктивних факторів, багато положень залишається цілком прийнятним для нашої держави. Звернувшись до досвіду країн ЄС, США, можна виокремити такі аспекти, які слід було б впровадити Україні для забезпечення кібербезпеки:

– побудова ефективної урядової моделі, спрямованої на забезпечення кібербезпеки;

– визначення адекватного механізму, в основному у вигляді суспільно-державного партнерства, який дозволить приватним та державним зацікавленим суб'єктам обговорювати та визначати політику у сфері забезпечення кібербезпеки;

– визначення цілей та способів розвитку державних можливостей, а також необхідної законодавчої бази для участі у міжнародній боротьбі з кіберзлочинністю;

– визначення ключових інформаційних інфраструктур, у тому числі – основних активів, сервісів та взаємозалежностей;

– підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв та розробка механізмів захисту для ключових інформаційних інфраструктур;

– розробка системного та інтегрованого підходу до державного управління ризиками;

– запровадження нової програми освіти, в якій буде зроблено акцент на навчання ІТ-фахівців та професіоналів в області кібербезпеки;

– розвиток міжнародної співпраці у зазначеній сфері [2].

Отже, удосконалення правової регламентації протидії кіберзлочинності в Україні має відбуватися з урахуванням національних культурно-історичних, соціально-економічних особливостей нашої держави на підставі детального наукового аналізу міжнародного законодавства та досвіду інших країн у сфері боротьби з кіберзлочинністю.

Література

1. Довбиш М. Кіберзлочинність в Україні. URL : https://www.science-community.org/ru/node/16132. (дата звернення 06.03.2019).

2. Государственные стратегии кибербезопасности. URL : http://www.securitylab.ru/analytics/429498.php. (дата звернення 06.03.2019).

3. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : від 28 січ. 2003 р. ; ратиф. Україною 21 серп. 2006 р. URL : http://zakon.rada.gov.ua/laws/show/994_687 (дата звернення 06.03.2019).

4. Конвенція [ООН] проти транснаціональної організованої злочинності : прийн. резолюцією 55/25 Ген. Асамблеї від 15 листоп. 2000 р. ; ратиф. із застереженнями і заявами законом України від 4 лют. 2004 р. № 1433-15. URL : [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/995_789 (дата звернення 06.03.2019).

5. Конвенция об информационном и правовом сотрудничестве, касающемся «Информационных общественных услуг» : ETS № 180 от 4 окт. 2001 г. URL : http://zakon.rada.gov.ua/laws/show/994_559 (дата звернення 06.03.2019).

УДК 004.056.57

Березньова А.О.
Національна академія Служби безпеки України
Козюра В.Д.
кандидат технічних наук, доцент,
Національна академія Служби безпеки України

ТАРГЕТОВАНІ АТАКИ: ФАЗИ ЗДІЙСНЕННЯ

На даний час технологія та ефективність сучасних систем виявлення кібернетичних атак значно залежить від моніторингу інформації про кіберзлочини, а також від оперативності їх виявлення. Щоб мати можливість протидіяти сучасним кібернетичним загрозам будь-якій системі захисту необхідно вміти швидко адаптуватися до змін. Незважаючи на появу досить потужних антивірусних пакетів, небезпека зараження комп'ютерів не лише не зменшується, але продовжує зростати.

Тому сьогодні як ніколи є актуальною тема захисту інформації, її користувачів, інформаційних ресурсів, каналів передачі даних від зловмисних дій.

Так, як найбільше інформації концентрується в комп'ютерах це змушує порушників шукати доступні шляхи викрадення потрібних даних. А для того, щоб розробити надійну систему захисту спочатку необхідно досконало вивчити принципи впровадження, роботи шкідливого програмного забезпечення.

Особливістю цілеспрямованих атак є те, що порушника цікавить конкретна компанія або державна організація, яка обробляє або зберігає інформацію, котра може бути використана злочинцями. Це відрізняє дану загрозу від масових хакерських атак – коли одночасно атакується велике число цілей і найменш захищені користувачі стають жертвою.

Цільова атака – це безперервний процес несанкціонованої активності в інфраструктурі атакованої системи, з віддаленим ручним керуванням та в реальному часі. Це деяка операція, а не просто разове технічна дія. Процес спрямований для роботи в умовах конкретної інфраструктури, покликаний подолати конкретні механізми безпеки, певні продукти, залучити у взаємодію конкретних співробітників [1, 2].

Зазвичай цією операцією управляє організована група професіоналів, діяльність яких може бути схожою на багатоходову військову операцію.

Інструментарієм цільових (таргетованих) кібератак є засоби APT (Advanced Persistent Threat – атакуюча безперервна загроза) – комбінація спеціальних утиліт видаленого доступу, шкідливого програмного забезпечення, механізмів використання вразливостей «нульового дня», а також інших компонентів, спеціально розроблених для реалізації конкретної атаки [2].

У процесі здійснення проведення цільовій атаки можна виділити наступні етапі [1, 2]:

І. Підготовка. Спочатку необхідно виявити цілі. В ході тривалого моніторингу групи порушників використовують загальнодоступні інструменти, такі як офіційні Twitter-акаунти компаній, профільні форуми, де обмінюються інформацією різними співробітники. Це допомагає визначити жертву і завдання атаки, після чого ресурси групи переходять до етапу активної розвідки. Потім відбувається безпосередній збір інформації. Жодна компанія не надає відомості про те, які технічні засоби вона використовує, в тому числі для захисту інформації, внутрішній регламент і т.д. Тому процес збору інформації про жертву називається розвідкою. Основне завдання розвідки – збір цільової приватної інформації про об’єкт атаки. Тут важливі всі дрібниці, які допоможуть виявити потенційні слабкі місця. У роботі можуть бути використані самі нетривіальні підходи для отримання закритих первинних даних, наприклад, соціальна інженерія.

Важливим підетапом є розробка стратегії. Стратегія є обов’язковою для реалізації успішної цільової атаки, вона враховує увесь план дій на всіх стадіях атаки:

- опис етапів атаки: проникнення, розвиток, досягнення цілей;
- методи соціальної інженерії, що використовують уразливості, обхід стандартних засобів безпеки;
- етапи розвитку атаки з урахуванням можливих позаштатних ситуацій;
- закріплення всередині, підвищення привілеїв, контроль над ключовими ресурсами;
- вилучення даних, видалення слідів, деструктивні дії.

ІІ. Проникнення. Це активна фаза атаки, що використовує комбіновану техніку соціальної інженерії й уразливостей «нульового дня» для первинного інфікування цілі та проведення внутрішньої розвідки. Після закінчення розвідки і визначення приналежності інфікованого хоста по команді порушника через центр управління може завантажуватися додатковий шкідливий код.

ІІІ. Поширення. Фаза закріплення усередині об’єкту критичної інфраструктури переважно на ключових комп’ютерах. При необхідності через центри управління вносяться необхідні корективи в шкідливий код на основі зібраної ключової інформації.

IV. Досягнення мети. Ключова фаза цільової атаки, залежно від вибраної стратегії в ній може застосовуватися внесення змін до технологічних процесів, що призводять до аварій та катастроф, розкрадання закритої інформації, умисне внесення змін до закритої інформації, маніпуляції з бізнес-процесами, розкрадання фінансових ресурсів.

Висновки. Активне поширення цільових атак обумовлено сильним скороченням вартості і трудовитрат в реалізації самої атаки. Цільова кібератака буде успішною, якщо сліди активності на усіх її етапах будуть приховані. Основна маса цільових атак проводиться через Інтернет. Для цього порушники можуть заразити сайт, який часто відвідують потенційні жертви, після чого відбувається зараження комп'ютерних систем і проникнення. Тому, захист від цільових атак - це комплексна задача, яку не можна вирішити використовуючи один який-небудь продукт інформаційної безпеки. Для досягнення мети потрібно застосовувати весь спектр засобів, тільки в цьому випадку можна підвищити відсоток успішного виявлення атак.

Література

1. Козюра В.Д. Як протистояти реальним кіберзагрозам об'єктам критичної інфраструктури України / В.Д.Козюра. [Електронний ресурс]. – Режим доступу: http://dspace.oduvs.edu.ua/bitstream/123456789/501/1/ilovepdf_com-79-80%5B1%5D.pdf.

2. Левцов В. Анатомия таргетированной атаки / В.Левцов, Н.Демидов; Журнал «Information Security/ Информационная безопасность», № 2, 2016, с. 36-39 [Електронний ресурс]. – Режим доступу : http://www.itsec.ru/articles2/Oborandteh/anatomiya-targetirovannoy-ataki, №3, 2016, с. 34-38 [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/articles2/Oborandteh/anatomiya-targetirovannoy-ataki-chast-2, № 4, 2016, с. 40-45 [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/articles2/Oborandteh/anatomiya-targetirovannoy-ataki-chast-3, № 6, 2016, с. 18-23 [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/articles2/target/anatomiya-targetirovannoy-ataki-chast-4.

УДК 004.62

Бржевська З.М.
Державний університет телекомунікацій

ВПЛИВ НА ДОСТОВІРНІСТЬ ЯК ЗАГРОЗА ДЛЯ ІНФОРМАЦІЇ

Сучасний інформаційний простір [2] є унікальною можливістю одержувати будь-яку інформацію з визначеного питання за умови наявності відповідного інструментарію, застосування якого дає змогу аналізувати взаємозв'язок можливих подій, які вже відбуваються, з інформаційною активністю певного кола джерел інформації. Виходячи із реалій сьогодення ефективна інформаційна політика держави залежить не тільки від надійності функціонування інформаційно-телекомунікаційних систем, а й у

значній мірі від захищеності її інформаційних ресурсів. Тому аналіз визначення достовірності інформації, об'єктів та суб'єктів інформації стануть першим кроком для розроблення такої методики, яка буде виявляти вплив на достовірність інформаційних ресурсів.

Розглянуто та проаналізовано визначення достовірності інформації, об'єктів та суб'єктів інформації, які стануть першим кроком для розроблення такої методики, яка буде виявляти вплив на достовірність інформаційних ресурсів. Під терміном достовірність інформації слід розуміти наближеність інформації до першоджерела та адекватне сприйняття об'єкта розгляду суб'єктами системи інформаційного простору. В якості об'єктів інформаційної безпеки виступають особа, суспільство та держава. Всі види інформації, які відповідають потребам суб'єкта, відповідають таким властивостям як конфіденційність, цілісність та доступність інформації [1]. Щодо впливу на інформацію та систему її обробки найбільший інтерес становлять загрози. Загроза в загальному вигляді буде представляти собою будь-який потенційно можливий несприятливий вплив на об'єкти, який (яка) завдає збиток суб'єкту інформаційної діяльності. Останнім часом значно поширився вплив на достовірність інформації, а отже з'явилося таке явище, як фальшива інформація. Для простого прикладу, це – новини, сторінки в соціальних мережах, підроблені під рейтингові сайти, за допомогою яких певні групи людей або окремі особи привертають увагу суспільства до недостовірних подій некоректним шляхом. Подібна інформація, зокрема, недостовірна, розповсюджуються з великою швидкістю, поступово поповнюючись новими подробицями, які є реакцією індивідуумів. Розглянуто шляхи появи недостовірної інформації. також надано рекомендації щодо виявлення недостовірної інформації. Зважаючи на те, що достовірність інформації залежить від самих видань, аналітикам слід звертати увагу на першоджерело, уважно вивчати факти, які лежать в основі інформації, ретельно перевіряти сумнівні відомості. Недостовірною дослідник має вважати інформацію, що надходить до інформаційного простору з «конфіденційних» джерел, навіть якщо матеріал містить посилання на організацію, яку представляє «джерело».

Щодо впливу на інформацію та систему її обробки найбільший інтерес становлять загрози. Під загрозою безпеки інформаційних ресурсів будемо розуміти дії, які можуть призвести до спотворення, несанкціонованого використання або, навіть, до руйнування інформаційних ресурсів. Таким чином, загроза в загальному вигляді буде представляти собою будь-який потенційно можливий несприятливий вплив (дію або бездіяльність) на об'єкти, який (яка) завдає збиток суб'єкту інформаційної діяльності.

З позицій впливу на інформацію та систему її обробки найбільший інтерес представляють загрози за метою реалізації. На їх підґрунті формується, як правило, формалізована модель оцінювання ступеня порушення системи захисту інформації у досліджуваній системі. Згідно з норматив-

ними документами ТЗІ України [3, 4] такі загрози полягають у порушенні конфіденційності, цілісності та доступності.

Такий параметр як достовірність інформації цілком визначається на методичному рівні розроблення інформаційних систем. Параметри достовірності обумовлюються більшою мірою також на методологічному рівні, проте на їх величину суттєво впливає і характер функціонування системи, передусім її надійність. При цьому параметри достовірності та своєчасності жорстко пов'язані з параметрами точності та актуальності.

Сучасний інформаційний простір, зокрема Інтернет, крім виконання функцій обміну думками та отримання інформації його користувачами в період інформаційного протистояння, стає об'єктом і засобом інформаційного керування. Серед користувачів мережі з'являються групи людей або окремі особи, які навмисно поширюють помилкову або спотворену інформацію.

Література

1 Бурячок В. Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа /. За заг. ред. докт. техн. наук, проф. В.Б. Толубко. – К. : ДУТ, 2015. – 288 с.

2 Грищук Р.В. Основи кібернетичної безпеки: моногр. / Р.В. Грищук, Ю.Г. Даник; під заг. ред. проф. Ю.Г. Даника. – Житомир: ЖНАЕУ, 2016. – 636 с.

3 НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»

4 НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»

5 Юдін О. Аналіз загроз державним інформаційним ресурсам / О. Юдін, С. Бучик. // Проблеми інформатизації та управління. – 2013. – №4. – С. 93–99.

6 Юдін О. Загрози державним інформаційним ресурсам: терміни та визначення / О. Юдін, С. Бучик. // Захист інформації. – 2014. – №2. – С. 121–125.

УДК 57.001

Бугай В.В.
Приходько А.Л.
Хмельницький О.О.
кандидат педагогічних наук,
Національна академія Служби безпеки України

СУЧАСНІ ПРОБЛЕМИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ НАСЕЛЕННЯ

З розвитком інформаційних технологій зростає важлива роль надійного захисту інформації. Захист конфіденційної інформації є досить актуальним в умовах розвитку електронної торгівлі, дистанційного навчання та

банківських операцій. Важливою проблемою захисту інформації є ідентифікація користувача, який отримує доступ до інформації з обмеженим доступом. Традиційний пароль має багато недоліків. Як альтернатива парольній системі або її доповнення розглядають ідентифікацію особи за біометричними даними. Біометрична перевірка має багато переваг над підтвердженням пароля, адже він легко може бути вкраденим, вгаданим або перехопленим зловмисником.

Біометричні параметри – вимірювальні фізичні характеристики або особистісні поведінкові риси, що використовуються для ідентифікації особи або верифікації наданої ідентифікаційної інформації про особу. Ідентифікація людини здійснюється відповідно до її фізіологічних властивостей. До них відносять: геометричну будову руки, відбитки пальців, малюнок сітківки та райдужну оболонку ока, портрет (інфрачервону карту людини), особливості мови, рукописний та комп'ютерний почерк. Ймовірність того, що знайдуться дві людини з однаковими ознаками дуже низька.

За допомогою сканера зображення відбитків пальця можуть виділяти характерні ознаки, які потім використовують для ідентифікації. Якщо роздільна здатність отриманого зображення складає 300-500 dpi, то на поверхні зображення пальця можна виділити велику кількість дрібних деталей, за допомогою яких можна їх класифікувати, але в системі ідентифікації використовують тільки два типа деталей візерунку :

- кінцеві точки – точки в яких закінчуються папілярні лінії ;
- точки розгалуження - точки в яких папілярні лінії роздвоюються.

Розпізнавання за сітківкою ока здійснюється з використанням інфрачервоного світла, направленого через зіницю до кровоносних судин на задній стінці ока.

За допомогою камери і спеціалізованого програмного забезпечення на зображенні особи виділяють контури брів, очей, губ, носа та обчислюються відстань між ними та інші параметри. Та багато інших технологій які слугують для розпізнавання особи.

За допомогою таких характеристик створюються біометричні документи,що посвідчують особу та електронний носій інформації на якому записано інформацію про біометричні дані особи з метою його ідентифікації. Такі документи є найбільш захищені від підробок та виключають користування ними іншими особами окрім власника. Відбувається суттєве підвищення захищеності населення від злочинності та проявів міжнародного тероризму.

6 грудня 2012 року набрав чинності Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус». Відповідно до цього Закону в Україні розпочато роботи із запровадження оформлення і видачі паспорта громадянина України, що містить безконтактний електронний носій із біометричними даними.

Література

1. « Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України , посвідчують особу чи її спеціальний статус» //Відомості Верховної Ради -,2013 -,№ 51. Ст. 716 Із змінами ,внесеними згідно із Законами № 1774-VIII від 06.12.2016 Ст. 25. № 2058-VIII від 23.05.2017. – ВВР. – 2017. – № 30. – Ст. 323.

2. А. Мороз « Біометричні технології ідентифікації людини. Огляд системи».

3. Біометрія як універсальний спосіб ідентифікації людини [Електронний ресурс]- Режим доступуhttp://ela.kpi.ua/.

УДК 004.056.53

Виноградов О.В.
Національна академія Служби безпеки України

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управління призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах, від несанкціонованого доступу. Захист інформації в комп'ютерних системах має низку специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаної з носієм, може легко і швидко копіюватися і передаватися по каналах зв'язку.

Відомо дуже велика кількість загроз інформації, які можуть бути реалізовані як з боку зовнішніх порушників, так і з боку внутрішніх порушників. Радикальне вирішення проблем захисту електронної інформації може бути отримано тільки на базі використання криптографічних методів, які дозволяють вирішувати найважливіші проблеми захищеної автоматизованої обробки та передачі даних.

При цьому, сучасні швидкісні методи криптографічного перетворення дозволяють зберегти вихідну продуктивність автоматизованих систем. Криптографічні перетворення даних є найбільш ефективним засобом забезпечення конфіденційності даних, їхньої цілісності і справжності. Тільки їх використання в сукупності з необхідними технічними та організаційними заходами можуть забезпечити захист від широкого спектру потенційних загроз.

Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи: перехоплення інформації - цілісність інформації зберігається, але її конфіденційність порушена; модифікація інформації - вихідне повідомлення змінюється або повністю підміняється іншим і відсилається адресату; підміна авторства інформації. Дана проблема може мати серйозні наслідки. Наприклад, хтось може надіслати листа від вашого імені (цей вид обману

прийнято називати спуфінга) або Web - сервер може прикидатися електронним магазином, приймати замовлення, номери кредитних карт, але не висилати ніяких товарів [2].

Автоматизована система – сукупність керованого об'єкта й автоматичних керуючих пристроїв, у якій частину функцій керування виконує людина. Автоматизована система являє собою організаційно-технічну систему, що забезпечує вироблення рішень на основі автоматизації інформаційних процесів у різних сферах діяльності (управління, проектування, виробництво тощо) або їх поєднаннях [1].

Результатом досвіду застосування мережі INTERNET є виявлена слабкість традиційних механізмів захисту інформації та відставання у застосуванні сучасних методів. Криптографія надає можливість забезпечити безпеку інформації в INTERNET і зараз активно ведуться роботи з впровадження необхідних криптографічних механізмів в цю мережу. Не відмова від прогресу в інформатизації, а використання сучасних досягнень криптографії - ось стратегічно правильне рішення.

Можливість широкого використання глобальних інформаційних мереж та криптографії є досягненням і ознакою демократичного суспільства. Володіння основами криптографії в інформаційному суспільстві об'єктивно не може бути привілеєм окремих державних служб, а є нагальною необхідністю для самих широких верств науково-технічних працівників, що застосовують комп'ютерну обробку даних або розробляють інформаційні системи, співробітників служб безпеки і керівного складу організацій і підприємств. Тільки це може служити базою для ефективного впровадження та експлуатації засобів інформаційної безпеки [3].

Література

1. Іванов А. О. Теорія автоматичного керування: Підручник. – Дніпропетровськ: Національний гірничий університет. – 2003. – 250 с.

2. Молдовян А.А., Молдовян Н.А., Рад Б.Я. Криптографія. - СПб.: Видавництво "Лань", 2001. – 224с. (Підручники для вузів. Спеціальна література).

3. Інформатика: Базовий курс / С.В. Симонович та ін. – СПб.: Пітер, 2002. – 640 с.

УДК. 342

Власенко В.М.
Національна академія Служби безпеки України

ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО ЯК ЕЛЕМЕНТ ГІБРИДНОЇ ВІЙНИ

Сучасний етап розвитку людства характеризується інтенсивною інформатизацією усіх сфер життєдіяльності. Удосконалення інформаційних

технологій зумовили революційні зміни в медіапросторі, розширили можливості інформаційного обміну та створили умови для ефективного впровадження надбань інформаційного суспільства в різних сферах діяльності людини. Бурхливий розвиток новітніх засобів зв'язку охоплює чимдалі ширшу аудиторію та усуває існуючі бар'єри комунікації. Зростання ефективності сучасних комунікаційних технологій та методів управління великими масами людей спричинило їх застосування на державному та міждержавному рівні, а також необхідність впровадження ефективної системи захисту власного національного інформаційного простору.

Водночас, стрімкий розвиток інформаційних технологій вивів на новий якісний рівень інформаційне протиборство як елемент гібридної війни.

Особливістю сучасної гібридної війни є відсутність конфліктів високої інтенсивності із залученням усіх видів і родів військ та запеклими боями. Натомість мають місце точкові диверсійні удари, короткочасні бойові сутички, теракти, вбивства цивільного населення та тотальна пропаганда як ефективний інструмент контролю за населенням.

Інформаційна агресія, як елемент гібридної війни, являє собою сукупність цілеспрямованих інформаційних впливів, що здійснюються з метою інформаційно-психологічного впливу як на населення країни-супротивника, так і на власне населення з метою легітимізації рішень керівництва країни-агресора. Ще однією ціллю інформаційного протиборства з боку агресора є заволодіння інформацією з обмеженим доступом, її несанкціоноване поширення, зміна або знищення для досягнення бажаної мети.

Основними методами інформаційного протиборства є блокування або перекручування змісту інформаційних потоків і процесів прийняття рішень опонентом. Виправдовуючи своє втручання у внутрішні справи України, Кремль спрямовує свою пропагандистську машину проти української влади, намагається дискредитувати євроатлантичний вибір нашої держави, твердить про проведення "каральної акції" на Сході України, "громадянську війну" в Україні, "захоплення влади націоналістичними угрупуваннями" та іншими страшилками з метою проведення власної інформаційної політики на теренах нашої держави та втягування України до сфери своїх геополітичних інтересів.

Особливістю психології людини є те, що перше повідомлення, як і перше враження, здійснює на аудиторію найсильніший вплив. Змінити думку аудиторії впливу, яка склалася внаслідок первинної інформації, особливо в сфері суспільно-політичних процесів, важче, аніж сформувати це ставлення. Вказана особливість взята на озброєння та активно використовується фахівцями у сфері інформаційних війн. В інформаційному просторі з'явилися нові сфери впливу – блоги, які вже засвідчили свою ефективність в інформаційних протиборствах. Для максимального охоплення

аудиторії та оперативного поширення інформації використовуються спеціально найняті інтернет-користувачі (т.зв. “тролі”), а також використовується спеціальне програмне забезпечення, що автоматично поширює визначену інформацію (т.зв. “боти”).

Новітні технології дозволяють країні-агресору більш ефективно формувати образ ворога за допомогою відеорядів, фейкових повідомлень, “свідчень очевидців” та ефекту “присутності”. З метою глибокого розділення аудиторії за принципом “свій-чужий” застосовується технологія нібито боротьби глибинних смислів, добра і зла, світла і темряви. Так, у російських ЗМІ це боротьба “руського мира” з “нацистами”, “бандерівцями” які нібито захопили владу в Україні.

Ще більші зусилля правлячими російськими колами спрямовуються на інформаційну обробку внутрішнього споживача. Ключові меседжі кремлівських пропагандистів, що спрямовані на російську аудиторію, насичені високопарними висловами на кшталт: “Росія – велична країна, яка має врятувати людську цивілізацію від моральної деградації та занепаду”, “Росія – взірець духовності, Захід – світ гріха і розпусти”, “Крим – наш” тощо.

Забезпечення інформаційної безпеки держави, як складової національної безпеки, потребує створення системи протидії інформаційним загрозам і захисту власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави, що зумовлено необхідністю протистояти агресії в інформаційній сфері. Основним завданням забезпечення інформаційної безпеки держави постає протидія впливу агресора на суспільство, свідомість і підсвідомість особистості, нав’язуванню з боку супротивника системи цінностей, поглядів, інтересів і рішень у життєво важливих сферах.

Пропагандистські можливості Росії знаходяться на високому рівні, що вимагає від нашої держави відповідного гострого, рішучого реагування та протидії із застосуванням новітніх комунікаційних технологій, захисту власного інформаційного простору та створення якісного національного інформаційного продукту.

УДК: 316.485.6:351.746.1(477)

Гельжинський А.Ю.
Національна академія Служби безпеки України

РОЛЬ ЗМІ В ІНФОРМАЦІЙНІЙ ПРОТИДІЇ ТЕРОРИЗМУ

Наряду із перевагами, інформаційно-технологічний прогрес створив нові потенційні загрози життєдіяльності як для окремої держави, суспіль-

ства та громадян, так і для світової спільноти в цілому. Зокрема це стосується тероризму, який адаптувався до основних тенденцій інформатизації суспільства. Темпи зростання кількості інформації випереджає її осмислення соціумом. Це розширює можливості терористичних організацій для дезорієнтації населення і маніпулювання свідомістю при підготовці та здійсненні терактів, а також по залученню нових прихильників [7].

Сучасні реалії демонструють, що інформаційна протидія є одним з найменш досліджених напрямів антитерористичної діяльності як в Україні, так і на міжнародному рівні.

На практиці інформаційний аспект боротьби з тероризмом передбачає лише реалізацію заходів захисного характеру. Реалізації активних заходів інформаційної протидії загрозам терористичного характеру законодавством України не передбачено.

Інформаційна протидія тероризму повинна забезпечуватися комплексною реалізацією системи заходів з профілактики і попередження тероризму, поінформованістю населення про небезпеку та масштаби тероризму, порядком їх дій у разі терористичної атаки, активним залученням громадянського суспільства до участі у протидії тероризму, зокрема шляхом використання інформаційних ресурсів та за допомогою засобів масової інформації (ЗМІ).

Необхідно відзначити, що ЗМІ, як один з інститутів громадянського суспільства, повинен стати стратегічним ресурсом держави у забезпеченні її інформаційної безпеки і стабільного функціонування. Важливою умовою успішної боротьби з тероризмом є створення інформаційного середовища, що дозволяє забезпечити високий рівень правової та інформаційної культури громадян, нівелювати вплив на громадськість «певних політичних, релігійних чи інших поглядів винного (терориста)» [1].

Чітко продумана інформаційна політика в ЗМІ дозволить не тільки уникнути негативного впливу і психологічної деформації населення, які обумовлені пропагандою насилля, вседозволеності, безкарності, але й забезпечить успішність проведення антитерористичних заходів, формування у суспільстві відчуття захищеності та розуміння порядку дій у випадку підвищення рівня терористичної загрози.

Поряд з цим, державі необхідно нарощувати активність в освоєнні нових каналів комунікацій, таких як інтернет-форуми, блоги, чати, які терористи вже давно використовують для просування вигідних їм ідей. При цьому необхідно враховувати особливості аудиторії та вміти вести дискусію на зрозумілій їй мові для адекватного сприйняття інформації [7].

Інформаційна протидія тероризму за допомогою ЗМІ повинна передбачати реалізацію комплексу заходів за такими напрямами:

- протидія пропаганді та поширенню ідеології тероризму в єдиному інформаційному просторі України [2,3];

•проведення серед населення інформаційно-роз'яснювальної та профілактичної роботи, спрямованої на неприйнятність тероризму та відмову від ідей використання терористичних методів для досягнення мети [2, 3], а також підвищення рівня інформованості суспільства про небезпеку та масштаби тероризму, поглиблення знань про феномен тероризму, тенденцій розвитку, історичних, культурних, національних та політичних умов виникнення цього явища;

•інформаційна робота з населенням з метою формування пильності, морально-психологічної стійкості, дисциплінованості, єдності та особистої відповідальності;

•формування громадської думки з метою ефективної реалізації державної політики у сфері боротьби з тероризмом та формування іміджу сильної держави, здатної протистояти терористичній загрозі;

•навчання населення правилам поведінки в умовах терористичних загроз;

•пошук, збір та аналіз інформації про діяльність терористичних організацій та їх членів;

•інформаційний вплив на терористичні організації, свідомість терористів, їх організаторів та пособників;

•чітка інформаційна взаємодія з суб'єктами антитерористичної діяльності.

Водночас, при висвітленні подій терористичного характеру і антитерористичної діяльності, ЗМІ повинні враховувати, що право людей на життя і безпеку є первинними по відношенню до права на свободу їх доступу до інформації та її розповсюдження [8].

Література

1. Кримінальний кодекс України // Відомості Верховної Ради України: кодекс від 05.04.2001, редакція від 26.02.2019[Електронний ресурс] – режим доступу: http://zakon3.rada.gov.ua/laws/show/2341-14.

2. Про Концепцію боротьби з тероризмом: указ Президента України від 25.04.2013 № 230/2013. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/230/2013.

3. Розпорядження Кабінет Міністрів України від 11.07.2013 № 547-р. «Про затвердження плану заходів з реалізації Концепції боротьби з тероризмом». [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/ 547.

4. Постанова Кабінету Міністрів України «Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків» від 18.02.2016 №92 (в поточній редакції від 16.05.2017, підстава 294-2017-п): [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/92-2016-п.

5. Актуальні питання протидії тероризму у світі та в Україні: аналіт. доповідь/ [Резнікова О.О., Місюра А.О., Дрьомов С.В., Войтовський К.Є.]; за заг. ред. О.О. Резнікової. – К.: НІСД, 2017. – 60 с.

6. Підготовка населення в сфері антитерористичної безпеки як один із шляхів підвищення ефективності боротьби з тероризмом/ О.В. Волошин, І.М. Рижов, С.С. Сігарьов//Наук. Вісн. НА СБ України. – 2015. - № 57. – с.121-127.

7. Партнерство государства, общественного сектора и делового сообщества в борьбе с тероризмом – безопасность через диалог, согласие и взаимодействие: материалы Международ. Науч.-практ. конф., Минск, 30-31 октября 2014 года: в 2 т./ Ин-т безопансоти Респ. Беларусь; редкол.: С.Н. Князев (гл. ред.) и др. – Минск, 2014. – Т. 1. – 204 с. + 4 с.

8. Партнерство государства, общественного сектора и делового сообщества в борьбе с тероризмом – безопасность через диалог, согласие и взаимодействие: материалы Международ. Науч.-практ. конф., Минск, 30-31 октября 2014 года: в 2 т./ Ин-т безопансоти Респ. Беларусь; редкол.: С.Н. Князев (гл. ред.) и др. – Минск, 2014. – Т. 2. – 296 с.

УДК 004.056.57

Герасименко В.В.
Козюра В.Д.
кандидат технічних наук, доцент,
Національна академія Служби безпеки України

ПРОБЛЕМИ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ВІД ТАРГЕТОВАНИХ АТАК

В основу дослідження покладено проблему захисту від таргетованих (цільових) атак на об'єкти критичної інформаційної інфрастуктури держави. Витонченість і технічна складність атак в цифровому просторі ускладнюється з кожним днем. У світі, де інформація стала одним з ключових ресурсів, її захист набуває критичної важливості.

Таргетована (цільова) кібератака є тривалим процесом несанкціонованої активності кіберзлочинів в умовах конкретного об'єкту критичної інфраструктури, покликаним здолати конкретні механізми забезпечення безпеки і завдати конкретного збитку (фізичного, інформаційного, морального і т.д.). Цей процес видалено керований в реальному часі організованою професійною групою кіберпорушників, озброєних потужними апаратно-програмними засобами [1].

Інструментарієм таргетованих кібератак є засоби APT (Advanced Persistent Threat – атакуюча безперервна загроза) – комбінація спеціальних утиліт видаленого доступу, шкідливого програмного забезпечення, механізмів використання уразливостей «нульового дня», а також інших компонентів, спеціально розроблених для реалізації конкретної атаки.

Що можна протиставити таргетованим кібератакам? [1-3]

1. Запобігання цільовим атакам – не допустити запуск неконтрольованих процесів в корпоративній мережі. Основні заходи:

- технічні рішення (захист кінцевих точок, міжмережеві екрани і системи запобігання вторгненням);
- навчання персоналу (ознайомлення з кіберзагрозами, тренування з кібербезпеці і т.п.).

2. Виявлення слідів атаки, розпізнавання ознак зараження. Для цього використовуються мережеві/поштові сенсори, що дозволяють здійснювати збір інформації з різних контрольних точок, сенсори робочих станцій, що дозволяють збільшити охоплення і деталізацію аналізованої інформації, компоненти динамічного аналізу об'єктів, центри аналізу аномалій, хмарні сервіси – обновлювані в реальному часі бази знань про загрози.

3. Реагування – реакція на інциденти інформаційної безпеки – застосування набору прийнятих процедур, спрямованих на мінімізацію збитку і усунення наслідків атаки. Етапи реагування включають ідентифікацію, заборону, лікування, відновлення, профілактику.

4. Прогнозування – реалізація проактивних заходів, що дозволяють істотно утруднити порушникам підготовку і проведення атаки. Етап прогнозування включає наступний набір послуг: тест на проникнення, оцінка рівня захищеності, своєчасна оцінка уразливостей, аналітичний звіт про загрози інформаційної безпеки.

Висновки. Рекомендовано почати з аналізу минулих атак і моделювання нападу на найбільш слабкі точки. Крім того в числі перших кроків з вибудовування захисту проти атак можна виокремити «принципу мінімальних привілеїв» – урізання прав користувачів до необхідного мінімуму.

Насамперед, потрібно реалізувати базовий набір засобів захисту – мова йде про міжмережеві екрани, антивірусний захист, системи захисту Web і E-mail, і паралельно – вести пропаганду комп'ютерної грамотності.

Література

1. Козюра В.Д. Як протистояти реальним кіберзагрозам об'єктам критичної інфраструктури України / В.Д.Козюра. [Електронний ресурс]. – Режим доступу: http://dspace.oduvs.edu.ua/bitstream/123456789/501/1/ilovepdf_com-79-80%5B1%5D.pdf.

2. Левцов В. Анатомия таргетированной атаки / В.Левцов, Н.Демидов; Журнал «Information Security/ Информационная безопасность», № 2, 2016, с. 36-39 [Електронний ресурс]. – Режим доступу : http://www.itsec.ru/articles2/Oborandteh/anatomiya-targetirovannoy-ataki, №3, 2016, с. 34-38 [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/articles2/Oborandteh/anatomiya-targetirovannoy-ataki-chast-2, № 4, 2016, с. 40-45 [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/articles2/Oborandteh/anatomiya-targetirovannoy-ataki-chast-3, № 6, 2016, с. 18-23 [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/articles2/target/anatomiya-targetirovannoy-ataki-chast-4.

3. Цифрова облога: Як захиститися від цільових кібератак [Електронни ресурс]. – Режим доступу: https://biz.nv.ua/ukr/kibervoiny_i_biznes/tsifrova-obloga-jak-zahistitisja-vid-tsilovih-kiberatak-1710843.html.

УДК 341
Гоц О.В.
старший викладач ННІ ІБ НА СБ України
Фасоль О.О.
студентка 4 курсу ННІ ІБ НА СБ України

ЩОДО НЕОБХІДНОСТІ ФОРМУВАННЯ КУЛЬТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасний технологічний процес дає підґрунтя для нових викликів інформаційній безпеці будь-якого підприємства не залежно від форми власності. І фізичні, і інформаційні активи повинні бути захищені від внутрішніх і зовнішніх загроз. Під загрозою інформаційної безпеки організації розуміється будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі [1]. Результатом таких загроз можуть стати як матеріальні збитки, так і зіпсована репутація компанії або навіть повне її знищення.

Таким чином, будь-яке підприємство, будучи частиною інформаційного суспільства, відчуває необхідність захисту одного з головних своїх активів - інформації. Такий захист не може бути ефективним, ґрунтуючись тільки на технічних рішеннях. Необхідно формувати на підприємстві загальну культуру інформаційної безпеки (далі - ІБ) : у кожного співробітника має бути відчуття цінності інформації, розуміння, навіщо і чому саме таким чином впроваджуються ті чи інші процеси інформаційного захисту, які часом бувають незручними для самих співробітників. Прищеплення такої культури може стати першим кроком у систематизації підходів і дій із захисту інформації на підприємстві. Навіть без технічних заходів впровадження культури ІБ само по собі знижує ризики в цій області.

На нашу думку культура інформаційної безпеки - це сукупність вироблених на підприємстві соціальних норм, установок, стереотипів поведінки та стандартизації які сприяють підвищенню ефективності роботи в організації та формують важливу складову набору організаційних методів захисту інформації в будь-якому сучасному підприємстві.

Цикл формування і підтримки культури інформаційної безпеки на підприємстві на думку незалежних експертів з інформаційної безпеки складається з наступних циклічних етапів [2]: інформування та навчання; контроль і виявлення порушень; проведення аудиту та внутрішніх розслідувань; дисциплінарний вплив.

Для ефективного формування корпоративної культури інформаційної безпеки підприємства необхідно виділити наступні методи:

1. Інформування та навчання (проведенні всіх видів інструктажу для співробітників підприємства з питань інформаційної безпеки у формі тре-

нінгів з використанням мультимедійних засобів; регулярному інформуванні співробітників по внутрішнім каналам організації матеріалами з ілюстраціями та позначками «терміново» або «важливо»; обов'язковому дистанційному навчанні співробітників з актуальних питань інформаційної безпеки у форматі електронного курсу з проходженням інтерактивних вправ, тестування, виконання практичних робіт в цікавій для них формі; популяризації теми захисту інформації (як на підприємстві, так і особистої інформаційної безпеки) шляхом направленням пам'яток або інформаційних брошур з ілюстраціями та яркою інфографікою з цікавими фактами для співробітників).

2. Контрольні заходи, які проводить служба захисту інформації, є важливим фактором, що впливає на рівень культури ІБ в організації. В даний час застосовуються різні способи контролю за забезпеченням режиму ІБ в організації, в т. ч. детально описані в нормативно-методичних документах та політиці безпеки підприємства

3. Проведення аудиту та комплексних розслідувань дозволяє відновити ланцюжок подій і виявити причинно-наслідковий зв'язок в діях працівників, є обов'язковою частиною циклу підтримки культури ІБ і сприяє розвитку як рядових працівників, так і співробітників служби захисту інформації в організації, оскільки вимагає від експертів високого професіоналізму і відповідальності.

4. Елементом моделі, які відповідають за зворотний зв'язок в класичному процесного підходу, виступає функціональний блок "Дисциплінарний вплив". У контексті формування та підтримки всередині організації культури ІБ, крім відомих і зрозумілих принципів "батога і пряника", даний елемент включає в себе розбір організаційних причин допущених порушень, який дозволить поліпшити діючі вимоги по ІБ; принцип "сарафанного радіо" на підприємстві дозволяє за мінімальний час донести важливу інформацію в зрозумілі вигляді до всіх співробітників організації; для нетехнічних працівників наявність професійної і зрозумілої оцінки від експерта в області захисту інформації стає додатково мотивуючим фактором до розвитку.

Зазначений перелік методів не є вичерпним. Проте потрібно пам'ятати, що при формуванні культури інформаційної безпеки у співробітників підприємства не повинно виникати відчуття обтяжливості, а методи роботи експертів із захисту інформації повинні приносити максимум користі та зацікавленості колективу.

Таким чином, формування культури інформаційної безпеки на підприємстві є одним із організаційних методів захисту інформації, який дозволяє на прикладному рівні мінімізувати ризики витоку інформації та протидіяти як зовнішнім так і внутрішнім загрозам інформаційним активам підприємства в цілому.

Література

1. Основні поняття. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. 1999 р.

2. Архипова И.С., Пантелеймонова Д.Ю. Формирование корпоративной культуры в области информационной безопасности // Современные научные исследования и инновации. 2017. № 4 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2017/04/81794 (дата звернення: 11.02.2019)

УДК 327.5:316.776.23

Даценко А.Ю.
Національний інститут стратегічних досліджень

АКТУАЛЬНІ МЕТОДИ ПРОТИДІЇ ДЕСТРУКТИВНИМ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ВПЛИВАМ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

Інформаційно-психологічні впливи РФ щодо України в умовах неоголошеної війни проводяться у тому числі шляхом застосування маніпулятивних та дезінформаційних технологій з метою формування вигідного для Росії сприйняття населенням України тих чи інших подій, історичних фактів щодо релігійної та національної ідентичності тощо.

Серед основних причин недостатньо ефективної протидії цим впливам експерти Національного інституту стратегічних досліджень зазначають:

– недостатньо захищений від неліцензованих трансляцій вітчизняний телерадіопростір, стабільне технічне покриття якого й досі є значно меншим за територію держави (навіть без урахування окупованих районів);

– недостатньо фахова, слабко організована й надто залежна від власників ЗМІ журналістська спільнота;

– критична кількість медіа, які, перебуваючи в інформаційному просторі України, порушують її закони та загрожують її національній безпеці;

– брак дієвих інституцій та механізмів оперативного реагування на інформаційні загрози як технічного, так і психологічного характеру [1].

Удосконалення методів захисту національного інформаційного простору від інформаційної зброї противника та послаблення його інформаційно-психологічного впливу є першочерговим завданням для здобуття перемоги в цій війні [2]. Досягнення перелому в українсько-російському інформаційному протистоянні можливе лише за умови успішного поєднання вертикальних і горизонтальних інформаційних обмінів у національному інформаційному просторі. Отже, йдеться про постійний вплив єдиного інформаційного комплексу під державним контролем.

З одного боку, даний процес сприятиме зміцненню вітчизняної інформаційної системи як суб'єкта міжнародних інформаційних відносин, що дуже важливо в умовах нинішнього інформаційного протистояння, а з іншого – забезпечуватиме внутрішню консолідацію суспільства як запоруку надійного загальносуспільного захисту національного інформаційного простору від негативних зовнішніх впливів.

Аналіз запропонованих у спеціалізованій та фаховій літературі заходів щодо захисту національного інформаційного простору від деструктивного інформаційного впливу РФ дозволяє виокремити такі основні напрями розвитку [3]:

– створення єдиного державного (міжвідомчого) органу, який здійснюватиме керівництво, координацію та контроль заходів щодо інформаційного протиборства, а також організацію взаємодії силових структур України з місцевими органами самоврядування, недержавними установами, громадсько-політичними організаціями, ЗМІ, тощо;

– удосконалення системи комплексного моніторингу матеріалів популярних аудіовізуальних та друкованих ЗМІ, а також Інтернет-ресурсів на предмет наявності ознак застосування маніпулятивних та дезінформаційних технологій;

– створення розгалуженої системи стратегічних комунікацій, здатної швидко й ефективно реагувати на сучасні інформаційно-психологічні впливи з урахуванням характеру і значущості цих впливів;

– формування та реалізація державної програми, спрямованої на підвищення в суспільстві рівня медіаграмотності (розуміння небезпеки від негативного інформаційно-психологічного впливу);

– продовження створення системи національного інформування для формування об'єктивної думки про події в Україні та за кордоном;

– удосконалення системи наукових досліджень у сфері інформаційної безпеки.

Як конкретні методи протидії інформаційно-психологічним впливам для захисту інформаційного простору фахівцями пропонуються [4]:

– встановлення та перекриття (знешкодження) потенційних каналів проникнення деструктивної інформації в національний інформаційний простір;

– пряме та непряме спростування джерела деструктивного впливу (сумнівність щодо джерела інформації; абсурдність звинувачень; прив'язка джерела інформації до будь-якої негативної події; введення ще одного негативного факту, який легко піддається спростуванню);

– відволікання уваги (відволікання ресурсів противника на інший об'єкт шляхом перенаправлення його на іншу діяльність; введення в інформаційний простір нового сенсаційного повідомлення; відвертання уваги аудиторії на малозначущий факт у рамках поточної проблеми);

– мовчання у відповідь;

– мінімізація впливу (акцентування на тому, що в повідомленні вказано на деякі правдиві події тощо);

– дискредитація (обнародування компромату; негативна «похвала»; невмотивоване освистування; громадське обурення);

– розмиття негативу (генерація нейтральної або позитивної інформації про об’єкт в об’ємах, що перевищують об’єми негативної інформації);

– доведення до абсурду (вироблення імунітету в аудиторії до негативу про об’єкт).

Література

1. Світова гібридна війна: український фронт : монографія / за заг. ред. В.П. Горбуліна. – К.: НІСД, 2017. – 496 с.

2. Технології розвитку і захисту національного інформаційного простору в умовах становлення сучасного інформаційного суспільства : наукова доповідь / Центр досліджень соціальних комунікацій НБУВ. URL: http://nbuviap.gov.ua/index.php?option= com_content&view=article&id=1747:tekhnologiji-rozvitku-i-zakhistu-natsionalnogo-informatsijnogo-prostoru&catid=78&Itemid=412 (дата звернення 7.03.2019).

3. Косогов О.М., Сірик А.О. Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на Сході України / О.М. Косогов, А.О. Сірик // Системи озброєння і військова техніка. - 2017. - № 1. - С. 38-41. URL: http://nbuv.gov.ua/UJRN/soivt_2017_1_7 (дата звернення 7.03.2019).

4. Вакуленко Р.В. Огляд та аналіз методів протидії інформаційним впливам супротивника в умовах інформаційної війни / Р.В. Вакуленко // Актуальні задачі та досягнення у галузі кібербезпеки. Матеріали Всеукраїнської науково-практичної конференції 23–25 листопада 2016 року, м. Кропивницький. - С. 186-187. URL: https://core.ac.uk/download/pdf/84825417.pdf (дата звернення 7.03.2019).

УДК 004.056.5

Діденко К.О.
Тимофєєв Д.С.
НТУ «Дніпровська політехніка»

ПІДХОДИ ДО СТВОРЕННЯ ПРОГРАМИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

На сьогодні, серед різноманітних видів оцінки поточного стану справ підприємства одним з пріоритетних для керівництва є аудит інформаційної безпеки. Виникають питання щодо захищеності інформаційної інфраструктури та відповідності нормативним документам, кращим міжнародним практикам, що довели свою ефективність. Саме аудит інформаційної безпеки є тим інструментом, що об’єктивно оцінює стан захищеності ін-

формаційних активів відповідно до певних критеріїв, стандартів, показників. В межах організації цю оцінку виконує внутрішній аудитор, на якого часто покладають відповідальність за створення власної програми аудиту інформаційної безпеки у зв'язку зі специфікою суб'єкта аудиту. Але, не дивлячись на те, що аудитори проходять сертифікацію для виконання такої роботи, їм все одно необхідна основа, від якої вони можуть відштовхуватися при створенні програми аудиту. Багато організацій публікують власні розроблені програми аудиту, тож, розглянувши їх, можна виділити підходи до створення цих програм, що будуть слугувати гарним підґрунтям.

Основним міжнародним стандартом, де визначені настанови з управління програмами аудиту, є ISO 19011:2018 «Керівні вказівки щодо здійснення аудитів систем управління». Цей стандарт може бути застосований до інших типів аудиту, включаючи аудит інформаційної безпеки, за умови врахування специфічних вимог до компетентності. У даному стандарті даються рекомендації щодо створення програми аудиту, що зможе включати в себе аудити, орієнтовані на один або декілька стандартів на системи управління, що проводяться окремо або комбіновано. Особливістю його є те, що він застосовує цикл організаційного управління PDCA (Plan–Do–Check–Act) до процесів управління програмою аудиту, що дозволяє аудитору вдосконалювати програму за допомогою вчасного виявлення неточностей та їх усунення [1].

Асоціація контролю та аудиту інформаційних систем ISACA також пропонує документ для створення власної програми аудиту – «Аудит інформаційних систем: інструменти та методи створення програм аудиту». Розробники даного документу виділяють, як найбільш важливий чинник для визначення цілей аудиту, розуміння аудитором бізнес-середовища та пов'язаних з ним ризиків. Особливістю даного документу є те, що він визначає п'ять кроків створення власної програми (визначення предмету, мети та обсягу аудиту, виконання попереднього планування та визначення процедур аудиту) та пояснює, що саме має слугувати джерелом інформації для кожного з кроків, що значно допомагає аудиторові систематизувати свою діяльність на кожному кроці [2].

Окрім загального оцінювання стану інформаційної безпеки, програма аудиту має враховувати специфіку діяльності підприємства, на якому проводиться аудит. В тих організаціях, де проводяться операції з використанням платіжних систем, аудитор має звернутися до вимог стандарту безпеки даних індустрії платіжних карток PCI DSS Ради зі стандартизації безпеки індустрії платіжних карток PSI SSC. Цей стандарт висуває вимоги до захищеності компонентів інфраструктури, в якій циркулює інформація про платіжні картки. Даний стандарт пропонує аудиторам, при створенні програми аудиту на етапі його планування, виконувати вибірку, що дозволяє полегшити процес оцінки стану захищеності при наявності великої кі-

лькості підрозділів та системних компонентів. Після процесу вивчення області та складності оцінюваного середовища, аудитор може самостійно зробити репрезентативну вибірку підрозділів організації та системних компонентів щоб оцінити відповідність організації вимогам PCI DSS. Також, згідно з цим стандартом, аудитор повинен документувати обґрунтування формування вибірок та процесів і механізмів, що використовувались для визначення розміру вибірки [3].

Якщо сталося, що організація обробляє персональні дані резидентів країн Європейського Союзу або має постійне представництво в ЄС, вона повинна відповідати правилам обробки персональних даних, що відображаються у Загальному регламенті із захисту даних GDPR. Аналізуючи цей регламент, можна сказати, що аудитор повинен включити до програми аудиту виконання процесу оцінки впливу на захист даних, під час якої визначаються операції над персональними даними, цілі обробки цих даних та вказуються ризики, що можуть виникнути під час обробки із заходами щодо їх мінімізації. Важливим є те, що GDPR точно визначає, що процес оцінки впливу на захист даних має проводитись ще до початку обробки персональних даних [4].

Отже, для створення власної програми аудиту інформаційної безпеки, аудитори можуть спиратися на міжнародні практики створення програм аудиту та на нормативні документи з інформаційної безпеки, що стосуються сфери діяльності підприємства. Це допоможе правильно організувати діяльність аудитора та скоротити час планування програми аудиту. Необхідно, також, пам’ятати, що аудит – не одноразова процедура, тому, при плануванні програми, необхідно враховувати періодичність перевірок та постійно слідкувати за змінами у сфері інформаційної безпеки для швидкого внесення виправлень або доповнень до програми.

Література

1. ISO 19011:2018 «Guidelines for auditing management systems». [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/70017.html

2. Information System Auditing: Tools and Techniques Creating Audit Programs. [Електронний ресурс]. – Режим доступу: https://www.isaca.org/KnowledgeCenter/Research/Documents/IS-auditing-creating-audit-programs_whp_eng_0316.PDF

3. Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures. [Електронний ресурс]. – Режим доступу: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1551799520693

4. General Data Protection Regulation. [Електронний ресурс]. – Режим доступу: https://gdpr-info.eu/

УДК 621.391.651.5
Жилін О.Т.
Гордієнко С.Б.
кандидат технічних наук, доцент,
Національна академія Служби безпеки України

РЕАЛІЗАЦІЯ КОНЦЕПЦІЇ МЕРЕЖІ УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЯМИ TMN

Мережі телекомунікацій є складними об'єктами управління, які потребують розподільної системи. Інтелектуалізація мереж телекомунікацій, що відбувається нині, потребує управління такими мережами за протоколами, незалежними від послуг, які, в свою чергу, можуть надаватися різними операторами та/або постачальниками (в тому числі конкуруючими) в межах усієї мережі незалежно від типів застосованих у ній технічних засобів. Така вимога може бути реалізованою лише за наявності системи управління [1].

Для взаємодії розподілених компонентів управління в єдиній системі, а також для реалізації нею функцій управління необхідна мережа, по якій передається інформація управління. Розуміння цього зумовило розробку концепції мережі управління телекомунікаціями TMN (Telecommunication Management Network) [2]. Мережа, будова якої ґрунтується на цій концепції, забезпечує функції управління мережами і послугами телекомунікацій, а також надає зв'язок між своїми складовими частинами, нею самою і телекомунікаційними мережами, послугами та іншими мережами управління телекомунікаціями (іншими TMN).

Принцип логічного відділення мережі управління телекомунікаціями TMN від власне мереж та послуг телекомунікацій, якими вона управляє, дають можливість здійснювати розподіл функцій TMN таким чином, що можна реалізовувати централізоване або децентралізоване управління. Тобто мережа управління телекомунікаціями дає змогу операторам телекомунікацій з кількох центрів здійснювати управління широкою номенклатурою розподіленого обладнання, мереж та послуг.

Кожну систему управління можна умовно поділити на дві основні частини – підсистему прийняття рішення та підсистему виконання рішень. Перша реалізується у вигляді програмно-технічних засобів технічної експлуатації. Враховуючи це, основний принцип TMN полягає в наданні організаційної архітектури для забезпечення взаємозв'язку різноманітних типів операційних систем та/або телекомунікаційного обладнання для обміну інформацією управління з використанням погодженої архітектури зі стандартними інтерфейсами, включаючи протоколи і повідомлення [2].

Мережа управління телекомунікаціями TMN може забезпечувати функції управління та зв'язок як між різними операційними системами, так і між операційною системою і єдиним елементом обладнання зв'язку до

складної мережі, що взаємопов'язує багато різноманітних типів операційних систем і обладнання телекомунікацій.

Концептуально мережа управління телекомунікаціями TMN є окремою мережею, що з'єднується з мережею телекомунікацій в окремих точках для взаємообміну інформацією з метою управління мережею телекомунікацій. Для своїх цілей вона може використовувати частини мережі телекомунікацій

Тут мережа управління телекомунікаціями для своїх потреб використовує канали та системи комутації мережі телекомунікацій. Межі мережі управління телекомунікаціями можуть змінюватися таким чином, щоб користувач (абонент) по TMN мав змогу управляти послугами телекомунікацій.

Через мережу управління телекомунікаціями TMN можна, наприклад, управляти:

- мережами телекомунікацій (загального користування і відомчими), у тому числі: цифровими мережами з інтегральним обслуговуванням, мережами зв'язку з рухомими об'єктами, віртуальними приватними мережами, інтелектуальними мережами;
- власне мережею управління телекомунікаціями;
- кінцевим обладнанням систем передачі (обладнанням групоутворення, волоконно-оптичними, радіорелейними, супутниковими);
- цифровими й аналоговими системами передачі (кабельними, волоконно-оптичними, радіорелейними, супутниковими);
- системами відновлення (резервування);
- операційними системами та їх периферійними засобами, кінцевими процесорами, груповими контролерами, серверами файлів тощо;
- глобальними, територіальними і локальними інформаційно-обчислювальними мережами (відповідно WAN – Wide Area Network, MAN – Metropolitan Area Network, LAN – Local Area Network);
- мережами з комутацією каналів і пакетів;
- кінцевим обладнанням і системами телефонної сигналізації, в тому числі транзитними пунктами сигналізації та базами даних у реальному часі;
- телематичними службами;
- відомчими АТС, точками доступу відомчих АТС та кінцевим обладнанням (терміналами) користувачів;
- терміналами користувачів цифрових мереж з інтегральним обслуговуванням;
- програмним забезпеченням, що надається телекомунікаційними службами, або зв'язаним з ним, наприклад, програмним забезпеченням систем комутації;
- прикладним програмним забезпеченням у межах центрального процесора, включаючи прикладне програмне забезпечення мережі управління телекомунікаціями TMN;
- допоміжними системами – випробувальним обладнанням, системами електроживлення, кондиціонерами, системами пожежної сигналізації та ін.

Мережу управління телекомунікаціями можна використовувати при управлінні розподіленими об’єктами, службами та послугами, що можуть бути комбінацією наведених прикладів.

У межах концепції TMN під управлінням також розуміється комплекс засобів та заходів, які дають можливість забезпечити обмін та обробку інформації управління з метою вдосконалення роботи Адміністрацій зв’язку. При цьому допускається мати необмежену кількість мереж управління телекомунікаціями в межах однієї Адміністрації зв’язку або об’єднану (єдину) мережу управління телекомунікаціями для кількох Адміністрацій зв’язку.

Служби і протоколи моделі взаємодії відкритих систем OSI (Open Systems Interconnection) [3] надають підкомплекс засобів управління, які можуть забезпечуватися за допомогою мережі управління телекомунікаціями. При цьому вона повинна мати інформацію про телекомунікаційні мережі і служби, як про сукупність взаємодіючих систем.

Слід зазначити, що розподілені середовища управління телекомунікаціями у цих випадках потребують об’єктно-орієнтованої розподіленої технології обробки інформації.

Література

1. Кривуца В.Г. Система управління сучасними телекомунікаційними мережами/ Кривуца В.Г., Беркман Л.Н. та ін. / - К.: Зв’язок, 2009. - 352 с.

2. Кривуца В.Г. Управління телекомунікаціями із застосуванням новітніх технологій:підручник для ВНЗ / В.Г.Кривуца, В.К.Стеклов, Л.Н.Беркман та ін. – К.: Техніка, 2007.- 384 с.

3. Стеклов В.К. Проектування телекомунікаційних мереж. підручник для ВНЗ / В.К.Стеклов, Л.Н.Беркман. – К.: Техніка, 2002. – 792 с.

УДК 355/359

Загребельний В.С.
Клочкова В.В.
Національна академія Служби безпеки України

ЮРИДИЧНІ ТА ІНФОРМАЦІЙНІ АСПЕКТИ ЗАСТОСУВАННЯ ПРОГРАМИ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ «НА ТЕБЕ ЧЕКАЮТЬ ВДОМА»

П’ять років минуло з того часу, як відбулася окупація з наступною анексією Автономної Республіки Крим без єдиного пострілу та розпочалась масова гібридна агресія Росії проти України на Донбасі. Попри численні факти участі Збройних сил РФ та докази причетності Росії до війни, офіційно Росія не визнає факту свого вторгнення в Україну, відтак з українського боку війна розглядається як гібридна [4].

Слід відмітити, що наша держава стала реальним об'єктом гібридних атак з боку Росії, оскільки засіб впливу охоплює всі елементи видів військових дій – гібридні, організаційні та мережеві, а саме: створення незаконних збройних формувань, економічний тиск, підтримка сепаратистів, пропаганда війни, численні кібератаки, використання соціальних мереж з метою дезінформації не тільки громадян України, але й всього світу [5].

Такі дії становлять, на сьогодні, реальну загрозу національній безпеці, територіальній цілісності України, а також її відносинам як на національному так і на міжнародному рівні.

Наразі російські медіа всіма можливими засобами намагаються пояснити вторгнення Росії на територію України і вдаються до перекручування фактів та відвертої брехні. Журналісти Росії намагаються запевнити власних глядачів, що в Україні процвітає хаос і безладдя, а ЗС РФ сприяли збереженню стабільності та захищали російськомовне населення [4, 5].

Утім, на сьогоднішній день, спираючись на оголошення Україною умов припинення вогню, Служба безпеки України в рамках спеціальної програми «На тебе чекають вдома» (далі – Програма) здійснює певні заходи щодо повернення на підконтрольну Україні територію та звільнення від кримінальної відповідальності громадян, які добровільно склали зброю та відмовилися від участі в діяльності незаконно створених збройних формувань так званих «ДНР/ЛНР», і не вчиняли тяжких та особливо тяжких злочинів [2].

Програма поширюється на осіб, які самовільно відмовились від участі в терористичних групах, не брали участі у вбивствах, тортурах, нападах на підприємства, установи та організації інших тяжких та особливо тяжких злочинах[2]. Юридичні підстави для звільнення від кримінальної відповідальності для учасників незаконних формувань «ДНР/ЛНР» передбачені ч. 2, ст. 258-3 («Створення терористичної групи чи терористичної організації»), ч. 6, ст. 260 («Створення не передбачених законом воєнізованих або збройних формувань») та іншими статтями Кримінального кодексу України [1, 2].

Станом на травень 2018 рік, дана Програма допомогла повернутися до мирного життя вже понад 308 нашим співвітчизникам [2].

Тож, щоб стати учасником цієї Програми, необхідно звернутись до співробітників Служби безпеки України безпосередньо або через родичів, знайомих за допомогою одного із доступних засобів зв'язку.

Слід зауважити, що Програма потребує визначення методів щодо її реалізації, тобто певний спосіб, за допомогою якого ця інформація надається потенційному колу суб'єктів. Найефективнішими шляхами розповсюдження відомостей є:

- буклети, листівки та рекламні щити (білборди);
- короткі фільми, відео;

- художні твори (вірші, проза);
- відеоряд з текстовим супроводом.

Кожен спосіб має свої переваги та недоліки, але для досягнення результату потрібне їх комплексне застосування, таким чином впливаючи на свідомість і підсвідомість осіб.

Перевагами цих способів є їх масовість та доступність розповсюдження, а саме: листівки та буклети поширюються за допомогою осіб, техніки, авіації, тощо; фільми, відео та відеоряд з текстовим супроводом за допомогою мережі Інтернет та телебачення, а художні твори – через радіомовлення. Найголовнішими критеріями оцінки даних методів є: яскравість та емоційність вираження, інформативність, стисліть викладу інформації, а головне зрозумілість. Тому, чим більше людей буде поінформовано про Програму, тим більше осіб матимуть змогу повернутися додому.

Отже, розпалювання Російською Федерацією конфліктів, створення осередків дестабілізації та зон військових дій свідчить про те, що «керований хаос» став основою зовнішньої політики Російської Федерації, а вторгнення її військ на територію України (не лише в Криму, а й на Донбасі) не викликає жодного сумніву – Росія веде проти України віроломну неоголошену війну [5].

Тому, можна стверджувати про важливість програми Служби безпеки України «На тебе чекають вдома», оскільки кожен має можливість виправити свої помилки та розпочати мирне життя без війни та насильства.

Література

1. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III // База даних «Законодавство України/ВР України».

2. Програма Служби безпеки України «На тебе чекають вдома» [Електронний ресурс]. – Режим доступу: https://ssu.gov.ua/ua/pages/206.

3. Війна на Сході України [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/Війна_на_сході_України.

4. Гібридна війна Росія проти України: уроки та висновки [Електронний ресурс]. – Режим доступу: https://www.ukrinform.ua/rubric-polytics/2107122-gibridna-vijna-rosii-proti-ukraini-uroki-ta-visnovki.html

5. Війна на Сході України. Війна на Донбасі [Електронний ресурс]. – Режим доступу: http://реферат.com.ua/referati/18-war/980-referat-na-temu-vijna-na-shodi-ukraini-vijna-na.html?start=1

УДК 004.056.53
Зибін І.Д.
Жевелєва І.С.
Національна академія Служби безпеки України

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ЖИТТЄВО ВАЖЛИВА СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

За умови сучасної ситуації, коли глобальних та регіональних інформаційних протистоянь, деструктивних впливів, зіткнення різноманітних національних інтересів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин. При зростанні технічного прогресу та цінності інформації буде все частіше ставитись питання щодо інформаційної безпеки людини, суспільства та держави. Тобто інформація стала чинником, який може призвести до значних технологічних аварій, військових конфліктів та поразок у них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів, і чим вищий рівень інтелектуалізації, інформатизації та технічного розвитку суспільства, тим потрібнішою стає надійна інформаційна безпека, оскільки реалізація інтересів, людей та держав все більше здійснюється за допомогою інформатизації [1].

Наразі під впливом спеціальних інформаційних атак може цілеспрямовано змінюватися мораль та свідомість окремих осіб та суспільства в цілому, нав’язуються шкідливі інтереси, мотиви, ідеології, спосіб життя, на перший план виходить аналіз сутності та форм сучасних методів скритого шкідливого впливу, вияву дій, що мають цілеспрямований шкідливий характер і які протирічать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах. Загроза національній безпеці держави в інформаційній сфері являє собою сукупність умов та чинників, які становлять небезпеку життєво важливим інтересам держави, суспільства і особи через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційнотехнічну інфраструктуру[3]

Доктрина інформаційної безпеки України, зазначає такі загрози інформаційній безпеці країни як, - поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ , а також мережу Інтернет; деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу,

суверенітету, територіальної цілісності та недоторканності України; прояви сепаратизму в ЗМІ, а також у мережі Інтернет за етнічною, мовною, релігійною та іншими ознаками. Однією із загроз національній безпеці України в інформаційній сфері є здійснення іноземними державами негативного інформаційно-психологічного впливу на суспільну свідомість громадян України та світову громадськість через проведення інформаційних акцій та кампаній, спеціальних інформаційних операцій. Недостатній контроль з боку держави за дотриманням законів України політичними силами, ЗМІ та окремими особами, які займаються підприємницькою діяльністю в інформаційній сфері, призводить до того, що нині трапляються непоодинокі випадки надання ефірного часу теле та радіопрограмам, спрямованим на руйнування моральних цінностей, свідомості української нації [3]. Інформаційна безпека нейтралізує та знешкоджує подібні прояви ворожої агресії. Інформаційна безпека визначається можливістю країни боротися проти таких впливів. Інформаційна безпека особистості характеризується рівнем і якістю її інформування щодо реального стану справ у всіх сферах життєдіяльності, захищеністю її психіки і свідомості від небезпечних інформаційних впливів – маніпулювання, дезінформування, тощо.

Варто наголосити, що проти України з боку Російської федерації ведеться гібридна війна, інформаційний аспект якої спрямован на нав'язування певних ідеологічних стереотипів, тієї чи іншої суспільної думки. Війни такого типу є досить поширеними у глобальному інформаційному просторі та їх всебічно досліджують науковці та фахівці. Одним із завданням інформаційної війни полягає у маніпулюванні масами. Метою такої маніпуляції є: внесення в суспільну та індивідуальну свідомість ворожих ідей та поглядів; дезорієнтація та дезінформація мас; послаблення певних переконань, залякування народу образом ворога; залякування супротивника власною могутністю [2].

Література

1. Баринов А. Информационный суверенитет или информационная безопасность? / А.Баринов // Національна безпека і оборона. – 2001. – № 1. – С. 70-76.

2. Богуш В.М. Інформаційна безпека держави / В.М.Богуш, О.К.Юдін. – К. : "МК-Прес", 2005. – 432 с.

3. Петрик В. Сутність інформаційної безпеки держави, суспільства та особ[Електронний ресурс]. – Режим доступу:http://www.justinian.com.ua/article.php?id=3222.

УДК 316.422
Казанцева С.С.
Національна академія Служби безпеки України

КІБЕРБЕЗПЕКА ЯК ОДНА ІЗ КЛЮЧОВИХ ПРОБЛЕМ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ

Сьогодні ми живемо в епоху інформаційного суспільства та є свідками науково-технічного прогресу, коли інформаційні технології і телекомунікаційні системи охоплюють усі сфери життєдіяльності як самої людини, так і держави загалом. Такий розвиток поступово трансформує світ, розширюючи таким чином свободу і можливості людей. Водночас такі переваги сучасного світу обумовили виникнення нових загроз національній та міжнародній безпеці.

Саме тому, можемо стверджувати, що кібербезпека – це нова ключова проблема сьогодення, оскільки з таким стрімким розвитком інформаційних технологій людство потребує захисту інформаційно-телекомунікаційних систем.

Такі провідні країни світу як Великобританія, Сполучені Штати Америки, Китай та інші, вже давно стикнулися з вищезгаданою проблемою та активно співпрацюють між собою у вказаному напрямку. У бюджеті цих держав давно закладаються величезні кошти на розвиток кібернетичної складової, а також регулярно забезпечується реалізація програм для забезпечення національної безпеки та захисту важливих державних об’єктів від кібератак. Слід відмітити той факт, що під час проведення зустрічі на вищому рівні глав держав та голів урядів країн-учасниць Північноатлантичного альянсу, яка проходила у 2016 році у Варшаві, було підписано перший в історії договір між ЄС та НАТО про співпрацю у сфері безпеки, зокрема в питаннях гібридних війн та кібератак [1].

Що стосується України, то в Законі України «Про основні засади забезпечення кібербезпеки України» розкривається поняття «кібербезпека» – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Особливо важливе значення кібербезпека відіграє для «діяльності, яка пов’язана із захистом інформації, що становить державну таємницю, а також для комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет» [2].

Ще одним ключовим документом у сфері кібербезпеки є Стратегія кібербезпеки України, прийнята у 2016 році. Це документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Для порівняння можемо зазначити, що Австрійська Стратегія кібербезпеки була ухвалена у 2013 році, у Франції у 2011 році, в Іспанії у 2013 році, у Великобританії в 2011 році, а Естонія є однією із перших країн у світі, оскільки ухвалила Стратегію кібербезпеки ще у 2008 році [1].

Стратегія кібербезпеки України має вагоме значення для національної безпеки України, оскільки в ній зазначаються «наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, підвищення ефективності основних суб'єктів забезпечення кібербезпеки, насамперед сектору безпеки і оборони, щодо виконання завдань у кіберпросторі [3].

Маючи системний і цілеспрямований характер, зовнішній негативний вплив призводить до появи загроз національній безпеці, які завдають державі суттєвих збитків. Особливо це стосується виконання завдань у сфері оборони країни, оскільки ця діяльність безпосередньо спрямована на захист національних інтересів держави від внутрішніх та зовнішніх загроз.

Слід зазначити, що в загальній системі кібербезпеки нашої держави одне з провідних місць займають саме Збройні Сили України. З початку 2014 року спостерігається тенденція до збільшення кількості кібератак різного ступеня складності, які направлені на порушення функціонування та дестабілізації обстановки в структурних підрозділах Збройних Сил України. Відповідними підрозділами поступово налагоджується взаємодія з суб'єктами забезпечення кібербезпеки в Україні. І сьогодні підрозділи ЗС України, які є відповідальними за кібербезпеку, вже перейшли на бойовий режим роботи у цій сфері, адже основним напрямком діяльності таких підрозділів є кібероборона держави.

Проведений аналіз свідчить про те, що сьогодні більшість кібератак здійснюються з території Російської Федерації, однак трапляються і випадки проведення кібератак з території інших країн-союзників, що, в свою чергу, ускладнює процес ідентифікації.

Таким чином, необхідно створити ефективну та надійну національну систему кібербезпеки; розширити функції та посилити можливості суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби з кіберзагрозами різного характеру; налагодити взаємодію обміну ін-

формацією між суб'єктами забезпечення кібербезпеки для прийняття спільних рішень та вироблення нових підходів для протидії кіберзагрозам. Також необхідно збільшити інвестування у кібербезпеку, розробляти правила, стандарти, положення, інструкції та інші нормативно-правові документи, які в подальшому допоможуть боротися з кібератаками та відповідати за їх скоєння. Для цього потрібно обмінюватися досвідом з провідними країнами, які вже є спеціалістами у даній сфері та запозичувати їх досвід для подальшого його впровадження в Україні.

Література

1. Кольцов М., Аушев Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні, – Лабораторія законодавчих ініціатив, 2017[Електронний ресурс]: – Режим доступу:http://parlament.org.ua/wp-content/uploads/2017/10/Policy-Paper_Kiberbezpeka.pdf.
2. Закон України «Про основні засади забезпечення кібербезпеки України».
3. Закон України «Про національну безпеку».
4. Закону України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]: – Режим доступу: https://zakon5.rada.gov.ua/laws/show/96/2016.

УДК 351.746.1

Капленко І.О.
Національна академія Служби безпеки України

ОСОБЛИВОСТІ НАЦІОНАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ В СУЧАСНИХ УМОВАХ

Останні роки української державності національний інформаційний простір набув певних особливостей, розуміння та врахування яких вкрай необхідно для формування сучасного інформаційного суспільства. Сьогодні очевидним є високий рівень зовнішніх загроз інформаційній сфері України, викликаних активною інформаційно-пропагандистською експансією інших країн, у першу чергу Російської Федерації (РФ).

У той же час слід констатувати, що дедалі більше деструктивних інформаційних впливів в Україні здійснюються на регіональному рівні, причому це притаманно не лише для територій, які традиційно є зонами пріоритетного інформаційного впливу російської пропаганди, а й для західних регіонів України, де, крім російського, посилюється інформаційна присутність і сусідніх держав. Питання історичної пам'яті, регіональної політики, забезпечення прав національних меншин дедалі частіше стають предметом маніпуляцій з боку інших держав, але так само і РФ, яка намагається їх використати у власних інтересах. Активізують свою, не завжди

дружню, інформаційну діяльність у прикордонних регіонах і інші сусідні держави.

РФ, Республіка Польща (РП), Угорщина і Румунія продовжують неофіційно поширювати ідеї щодо федералізації України, дискредитації представників органів державної влади та правоохоронних органів України. Суміжними державами реалізуються заходи щодо збільшення протестного потенціалу та автономізації окремих регіонів України на етнічному підґрунті. Отже, кожний регіон нашої держави перебуває під різними інформаційними впливами.

Активно розвивається мережа польських засобів масової інформації (ЗМІ) в Україні. В українсько-польських ЗМІ, що діють в Україні, здійснюється популяризація сусідньої країни, окрім суспільно-політичної ситуації в РП та Україні, чимала увага приділяється польським навчальним програмам, студентському обміну, роз'ясненням щодо працевлаштування в Польщі та отримання "карти поляка", тощо.

Польською стороною за допомогою мережі Інтернет цілеспрямовано підтримується історична пам'ять про колишню належність "Великій Польщі" нинішньої Західної України. Це стосується населених пунктів Тернопільської області (міста Тернопіль, Чортків, Кременець, Теребовля, Гусятин) і деяких інших міст України, зокрема Львова, Івано-Франківська, Луцька. Для наочності описання ілюструються географічною картою станом на 1939 рік. Аналогічно надається інформація і про українське місто Кременець, із органами місцевого самоврядування якого було укладено договір про двостороннє співробітництво польською стороною – містом Констанцин-Єзьорна, Пясечинський повіт, Мазовецьке воєводство [1].

Загрозливою щодо України вбачається й інформаційна політика Угорщини. Відповідно до положень Стратегії національної політики Угорщини до 2020 року [2], затвердженої угорським урядом, одним із пріоритетних завдань визначається створення єдиної інформаційної системи на території Закарпатської області, спрямованої на формування національної свідомості "зарубіжних угорців", та мобілізація можливостей цієї соціальної групи в інтересах національної політики офіційного Будапешта.

Ситуація суттєво ускладнюється ідеологічно-пропагандистською діяльністю "русинських організацій", поширення ними пропагандистських матеріалів через ЗМІ та в мережі Інтернет, в яких обґрунтовується відокремленість регіону від України у контексті походження національностей в регіоні.

Чималий інформаційний тиск на території Закарпатської, Одеської та Чернівецької областей здійснюється з боку Румунії, зокрема – у контексті об'єднання етнічних румун і молдаван у складі "єдиної румунської нації". Так, декілька років тому в Молдові прорумуньскою асоціацією "Честь, гідність і Батьківщина" було здійснено інформаційну кампанію "Караван

об'єднання", спрямовану на пропагуванням приєднання румунських меньшин до Румунії та відновлення Великої Румунії.

Потребує уваги деструктивна позиція деяких румунських ЗМІ, що пропагують ідеї розпаду української держави, публікують матеріали із закликами до насильницької зміни територіального устрою України. Зокрема, в румунській газеті "Adevarul" неодноразово друкувалися матеріали з прогнозами громадянської війни в Україні та розділення нашої держави на проєвропейський захід і проросійський схід. Також порушувалося питання готовності Румунії втрутитися у конфлікт задля захисту румун Північної Буковини і Південної Бессарабії .

Отже, сучасне суспільство – з його інформаційними та комунікаційними технологіями, – суть інформаційного простору. В його межах здійснюється прихований чи відкритий цільовий інформаційний вплив, метою якого є досягнення певного результату – політичного, економічного, ідеологічного [3].

Водночас інформаційний простір є і інструментом досягнення певної мети, і реципієнтом інформаційних потоків. Як вже зазначалося, необхідний рівень інформаційної безпеки гарантується комплексом заходів (нормативно-правових, організаційних, технічних), спрямованих на запобігання, виявлення й нейтралізацію тих обставин, факторів і дій, які можуть завдати збитків чи зашкодити реалізації інформаційних прав, потреб та інтересів країни і її громадян.

Література

1. Константин-Єзьорна, Пясечинський повіт, Мазовецьке воєводство [Електронний ресурс]. – Режим доступу : www.konstancinjeziorna.pl/nasza-gmina/miasto-i-gmina/wspolpraca-zagraniczna/miasta-partnerskie/krzemieniec-ukraina.

2. Угорська національна політика. Рамки стратегії національної політики [Електронний ресурс]. – Режим доступу : https://zahidfront.com.ua/news/Ugorske-Zakarpattya.

3. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : моногр. / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – К. : Інтертехнологія, 2009. – 164 с.

УДК 004.056.5

Киричок Р.В.
Державний університет телекомунікацій

ГОСТРА НЕОБХІДНІСТЬ В НАВЧАЛЬНИХ КІБЕРАТАКАХ НА КРИТИЧНО ВАЖЛИВІ ОБ'ЄКТИ КРАЇНИ

В даний час глобальний розвиток і повсюдне впровадження критично важливих комп'ютерних систем (КВКС) в ядерні, енергетичні, авіаційні, телекомунікаційні та промислові підприємства, а також їх реалізація на

об’єктах інфраструктури великих мегаполісів різних держав світу призводить до появи нових цілей, які піддаються безлічі кібератак. При цьому, кількість, складність реалізації атак (особливо apt-атаки, коли зловмисники можуть залишатися непоміченими тривалий час викрадаючи значні об’єми даних або завдати шкоди в годину «Х») і розмір спричинених в результаті збитків, зростає з кожним роком, про що свідчать щорічні звіти провідних компаній з розслідування кіберінцидентів та аналізу ризиків інформаційної безпеки (ІБ), таких як Kroll [1], Verizon [2]. Це загострює необхідність в створенні та удосконаленні тих же систем виявлення і запобігання вторгнень (систем об’єктивного контролю захищеності), а також організації структурованих підрозділів (CERT, CSIRT), функціонування яких буде направлено на постійне відстежування появи нових кіберзагроз, вразливостей технічних компонентів, програмного забезпечення і навіть слабкостей людського фактору (у випадках застосування різноманітних технік соціальної інженерії), швидке реагування та оперативне їх усунення.

Недосконаліть існуючих методів та засобів кіберзахисту і відповідно низький рівень захищеності більшості КВКС з виходом в Інтернет, а також динамічно мінливий характер кібератак та недостатня кількість висококваліфікованих фахівців, можуть призвести до формування небезпечного стану функціонування критично важливих об’єктів держави. До того ж, сьогодні в ролі атакуючої сторони виступають не просто поодинокі «хакери» або їх угрупування, а цілі терористичні організації і навіть кібервійська протиборчих країн або країн потенційних супротивників, які ставлять під загрозу безпеку КВКС в формі шпигунства, саботажу, відмови в обслуговуванні. Про це свідчать, безпосередньо, заяви щодо суттєвого збільшення кібератак на критичну інфраструктуру (переважно в сферах енергетики, водопостачання, транспорту, зв’язку та банківській галузі) від спецслужб різних держав, як от наприклад: Служба безпеки України [3], BSI (Федеральне управління з ІБ – Німеччина) [4], NCCIC (Національний центр інтеграції кібербезпеки і комунікацій – США) [5].

Таким чином, завдання постійного моніторингу, своєчасного виявлення критичних вразливостей, оцінки захищеності КВКС та миттєвого реагування на кібератаки все ще залишаються актуальними. Однак, в першу чергу, необхідно виділити саме аналіз вразливостей та оцінку рівня захищеності як основу для попередження кібератак. При цьому, використання лише методів аналітичних обчислень та імітаційного моделювання, які використовуються при проектуванні КВКС – є недостатнім, оскільки саме під час їхньої експлуатації виникає набагато більше загроз ІБ (як мінімум, з часом виникає необхідність в оновленні КВКС, що нерідко призводить до появи критичних вразливостей). І тому бажано використовувати як пасивні (аналіз записів журналів реєстрації подій безпеки), так і активні (тестування на проникнення) методи аналізу вразливостей і оцінки рівня захищеності КВКС під час їхньої експлуатації. І якщо пасивні мето-

ди ще можна впевнено використовувати, то використання активних методів може, або надати неповноцінну картину через встановлені рамки тестування, або призвести до плачевних наслідків у випадку критичних помилок чи збоїв системи.

В результаті, існує гостра необхідність в щонайшвидшому створенні і розгортанні, на базі технологій віртуалізації та резервного копіювання, як університетських так і національних тренувальних симуляторів – кіберполігонів. В свою чергу, університетські надаватимуть можливість імітування кібератак на КВКС з одночасним відпрацюванням студентами, дослідниками або спеціалістами тактик відбиття цих атак. Національні ж – повинні будуть надавати можливість створення масштабованої моделі глобальної мережі Інтернет для проведення військових кібернавчань та відпрацювання технологій протидії таким явищам як кібертероризм та цілеспрямована атака з боку вороже налаштованих країн. Що в комплексі дозволить нашій державі вдосконалювати методи та засоби забезпечення інформаційної і кібернетичної безпеки, готувати висококваліфікованих фахівців й тим самим підтримувати на високому рівні захищеність об'єктів критичної інфраструктури України.

Звісно ж необхідно відмітити, що перші кроки були зроблені і на рівні університетів вже повноцінно функціонують декілька кіберполігонів, зокрема в Держаному університеті телекомунікацій та Київському університеті імені Бориса Грінченка, однак на національному рівні ще й досі немає жодного подібного проекту, лише згадка [6], в травні 2018 р., про початок реалізації пілотного проекту зі створення кіберполігону Збройних сил України (на кшталт National Cyber Range, який до речі був розгорнутий ще в 2012 р. в США).

Література

1. Global Fraud & Risk Report 2017/18 // Kroll. – 2018. – № 10.
2. Data Breach Investigations Report // Verizon Enterprise Solutions. – 2018. – № 11.
3. Партнерські спецслужби розкрили кібератаки РФ на веб-ресурси Організації із заборони хімічної зброї - СБУ [Електронний ресурс] – Режим доступу до ресурсу: https://ssu.gov.ua/ua/news/1/category/2/view/5292#.MGWXHjIl.dpbs.
4. Ausländische Hacker nehmen Stromversorgung ins Visier [Електронний ресурс] – Режим доступу до ресурсу: https://www.welt.de/politik/article188864277/Cyberangriffe-Wasser-und-Stromversorgung-im-Visier-internationaler-Hacker.html.
5. Критическая инфраструктура не в лучшем состоянии [Електронний ресурс] – Режим доступу до ресурсу: https://threatpost.ru/report-a-grim-reminder-of-state-of-critical-infrastructure-security/18458/.
6. НАТО допомагає Україні створити кіберполігон ЗСУ [Електронний ресурс] – Режим доступу до ресурсу: https://www.unian.ua/politics/10137197-nato-dopomagaye-ukrajini-stvoriti-kiberpoligon-zsu.html

УДК 343.1
Ковмир С.В.
Національна академія Служби безпеки України

РИЗИК-МЕНЕДЖМЕНТ У ПРОЦЕСІ РЕАЛІЗАЦІЇ ЗАХИСТУ УЧАСНИКІВ КРИМІНАЛЬНОГО СУДОЧИНСТВА

У сучасному світі керування ризиком будь-якої діяльності є однією з основних складових загальної системи управління. Усвідомлення практичного значення керування ризиком у правоохоронній сфері активізувало в останні десятиліття дослідницький інтерес до цієї проблематики. Здатність постійно відслідковувати можливі несприятливі зміни ситуації, тримати їх під контролем, адекватно реагувати належить до числа найважливіших стратегічних переваг індивіда, групи та колективу.

Суб'єктивність інформації про загрозу учаснику кримінального судочинства та відсутність чіткого диференціювання відповідно до рівня загрози, його психологічного стану, або потенційної загрози, яку він може становити для оточуючих, створює неабиякі труднощі для підрозділу захисту під час вибору конкретного заходу забезпечення безпеки. Один із прийомів, що підвищують ймовірність успіху в таких умовах, - використання методів керування ризиками.

Треба визнати, що показання свідків у кримінальних провадженнях, пов'язаних з організованою злочинністю та тероризмом, відіграють ключову роль у формуванні всієї доказової бази. Відсутність надійної функціонуючої системи захисту свідків в Україні призводить до відмови деяких з них свідчити у кримінальних провадженнях. Вбивство осіб, які сприяють встановленню істини, на жаль вже стали буденними в українському суспільстві. Ресурси правоохоронних органів в цій сфері вкрай обмежені, а заходи безпеки, які здійснюються щодо цих осіб, не дозволяють задовольнити потреби системи правосуддя в необхідному обсязі.

Концепція системного ризик-менеджменту має бути заснована на ідеології спільної зацікавленості всіх структурних підрозділів системи захистуучасників кримінального судочинства в доцільному об'єднанні організаційних, матеріальних, інтелектуальних та інших ресурсів. Потреба в такому об'єднанні визначається цілями виявлення, передбачення та оцінки всієї динамічної сукупності ризиків, що стосуються свідка,а також оптимальним та своєчаснимреагуванням на загрози, що виникають.

Реалізація заходів захисту, особливо якщо вони пов'язані із забезпеченням безпеки учасників кримінального судочинства не є детермінованим процесом. Динамізм технологічного прогресу, варіативність загроз, складність та небезпечність виконуваних завдань, відсутність, часом у

співробітників підрозділів захисту, необхідної кваліфікації - через ці та багато інших факторів заходи захисту часто здійснюються не так, як планувалося заздалегідь.

Слідчі, прокурори або судді вимушені робити таку «оцінку» на основі, винятково, власного досвіду та інтуїції, зазвичай просто не маючи фізичного часу для встановлення ступенязагроз та вірогідності їх реалізації через можливості оперативних підрозділів. Треба також визнати, що навіть за наявності певних термінів для здійснення такої перевірки, оперативні підрозділи не мають науково обґрунтованих сучасних методик та відповідних фахівців для вирішення питання оцінки імовірних ризиків для свідків (фізичних, психологічних, юридичних, фінансових, ІТ-ризиків).

На жаль в Україні керування ризиками в цій сфері правоохоронної діяльності наразі майже не використовується, забезпечення безпеки учасників кримінального судочинства здійснюється, як правило, в «пожежному» режимі. Певна організаційна складність процесів захисту, відсутність кваліфікованого аналітичного персоналу, консервативність правоохоронної системи в цілому – не дозволяє в повній мірі використовувати подібні методики в Україні.

Водночас, орган, який безпосередньо має реалізовувати заходи забезпечення безпеки щодо свідка, у разі прийняття рішення про включення його до програми захисту, міг би використовувати результати оцінки цих ризиків (початкового та періодичного) для ефективного та раціонального задіяння наявних у нього сил та засобів (наприклад, при низькому рівні загрози – «забезпечення конфіденційності відомостей про особу» в матеріалах кримінального провадження; середньому – «використання технічних засобів контролю та візуальне спостереження», високому – «особиста охорона, переселення в інше місце проживання» тощо). До керування ризиками щодо свідків мають залучатися професійні психологи, ІТ-спеціалісти, фахівці логістичної сфери, оперативники з досвідом створення відповідних нових «легенд» для свідків щодо яких прийнято рішення про зміну персональних даних та переселення тощо.

Покращення професійного рівня спеціалістів підрозділів захисту, взаємодії з оперативними та слідчими підрозділами дозволить динамічно вдосконалювати систему захисту учасників кримінального судочинства. Співробітники підрозділу захисту свідківмають усвідомити, що не вся, необхідна для прийняття рішення щодо забезпечення безпеки інформація, є заздалегідь відомою, що існують оптимістичні і песимістичні сценарії розвитку подій. Члени команди захистумають розуміти, що кожен їхній вибір може потенційно вести до певних втрат і це допомагає їм обирати найбільш оптимальне рішення. Керування ризиками виходить за межі загального планування операціями захисту тамає стати могутньою зброєю у реалізації заходів захистуучасників кримінального судочинства в Україні.

Література

1. Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві: Закон України від 4 квітня 1994р. // Відомості Верховної Ради України. – 1994. – № 11. – Ст. 51.
2. Earley, P.& Shur, G. WITSEC: Inside the Federal Witness Protection Program. Bantam Book, February 2002, 485p.
3. UNODC. Good practices for the protection of witnesses in criminal proceedings involving organized crime. New York: United Nations, 2008.
4. http://www.m-economy.ru/art.php?nArtId=1652.
5. http://citforum.ru/SE/project/risk/.

УДК 340.132:[351.746.1+004.9]

Ковтун А.С.
Науково-дослідний інститут
інформатики і права НАПрН України

ЩОДО ПИТАННЯ ПРО ВИЗНАЧЕННЯ ПОНЯТТЯ «ІНФОРМАЦІЙНА АГРЕСІЯ»

Глобальний розвиток інформаційних технологій та впровадження їх в суспільне життя спричинили не лише формування інформаційного суспільства, але потребу в його захисті від негативного прояву їх використання. Сучасні деструктивні впливи на соціально-значущі відносини держави здійснюються переважно з використанням інформаційних технологій. Одним із таких деструктивних впливів є інформаційна агресія. Даний термін став все частіше вживаним за останній час.

Питанням захисту інформаційної безпеки держави, включаючи від інформаційної агресії, приділено значну увагу у наукових працях І.В. Авдошина, Ю.І. Дем'яненко, В. М. Желіховського, С.Я.Довбні, О.Д. Довганя, С.В. Дрьомова, І.Ф. Коржа, А.Ю. Нашинець-Наумової, В.Г. Пилипчука, В.М. Фурашева та інших науковців.

Через недостатній стан захищеності інформаційного суспільства, на сьогодні, потребуються рішучі кроки держави щодо визначення та закріплення на законодавчому рівні заходів спрямованих на подолання негативних явищ в інформаційному просторі.

На даний час визначення поняття «інформаційна агресія» не закріплено на законодавчому рівні.

Поняття «інформаційна агресія» вперше згадується в Рішенні Ради національної безпеки і оборони України від 24 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». Зокрема, в Рішенні вказано: «Кабінету Міністрів України розробити і внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України щодо

протидії інформаційній агресії іноземних держав, передбачивши, зокрема, визначення механізму *протидії негативному інформаційно-психологічному впливу*, в тому числі шляхом заборони ретрансляції телевізійних каналів...» [1].

З вищезгаданого Рішення можна дійти висновку, що законодавець визначає інформаційну агресію як негативний інформаційно-психологічний вплив.

Також, «інформаційна агресія» згадується в Указі Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» як актуальна загроза національним інтересам та національній безпеці України в інформаційній сфері. Оскільки, інформаційна агресія вважається як актуальна загроза національним інтересам та національній безпеці, то її визначення має бути закріплено в Законі України «Про національну безпеку України» [2].

У науці інформаційного права приділено небагато уваги для визначення сутності і значення інформаційної агресії. Зокрема, А.Ю.Нашинець-Наумова визначає інформаційну агресію як маніпулювання інформацією, що провокує порушення цілісності суспільства, його стабільного, в тому числі емоційного, стану, підрив цілей, поглядів і світогляду населення, а також розпалювання конфліктів (міжособистісних, етнічних, міжнародних) [3, с. 67].

А також, поняття «інформаційна агресія» визначено як незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на нанесення супротивнику конкретної, відчутної шкоди в окремих областях його діяльності шляхом обмеженого та локального по своїх масштабах застосування сили [4].

Перш за все, для визначення поняття «інформаційна агресія» необхідно звернутися до тлумачення саме слова «агресія». Згідно Академічного тлумачного словника, агресія – неспровокований збройний напад однієї держави на іншу з метою загарбання її території, ліквідації або обмеження її незалежності [5].

Якщо визначати поняття інформаційної агресії враховуючи тлумачення «агресія» Академічного тлумачного словника, то «збройний напад», у сучасній трансформації, є інформаційна зброя як різновид зброї, з такими головними елементами інформацією та інформаційними технологіями.

Враховуючи вищенаведене, можна сформувати власне визначення поняття «інформаційна агресія». Зокрема, інформаційною агресією можна вважати цілеспрямований, негативний, інформаційно-психологічний вплив на суспільство та державу з метою завдання шкоди національним інтересам та безпеці шляхом поширення недостовірної, неповної, упередженої інформації.

Література

1. Рішення Ради національної безпеки і оборони України від 24 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» / Офіційний сайт Верховної Ради України. – [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/n0004525-14.

2. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» / Офіційний сайт Верховної Ради України. – [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/47/2017.

3. Нашинець-Наумова А. Ю. Інформаційна агресія як основний компонент інформаційної війни // Підприємництво, господарство і право. – 2015. – № 6. – 67 с.

4. В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. – К.: КНТ, 2006. – 280 с. (Серія: Національна і міжнародна безпека).

5. Академічний тлумачний словник – [Електронний ресурс]. – Режим доступу : http://sum.in.ua/s/aghresija.

УДК 366.56 (075.8)

Когут В.Є.
Тугарова О.К.
кандидат юридичних наук, доцент,
Національна академія Служби безпеки України

ПРОТИДІЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОМУ ВПЛИВУ В ПІДПРИЄМНИЦЬКІЙ ДІЯЛЬНОСТІ

Безпека підприємства – це стан стійкої життєдіяльності, за якого забезпечується реалізація основних інтересів і пріоритетних цілей підприємства, захист від зовнішніх і внутрішніх дестабілізуючих факторів незалежно від умов функціонування. Зважаючи на надане визначення, можна зробити висновок, що основною метою забезпечення безпеки підприємництва є нейтралізація та ліквідація загроз належному здійсненню підприємницької діяльності в Україні, у результаті настання яких можуть бути нанесені підприємствам усіх форм власності збитки або упущено отримання вигоди.

Однією із складових безпеки підприємництва є інформаційна безпека. Проте, у сучасній науці визначенню змісту поняття «інформаційна безпека підприємництва» приділяється незначна увага, свідченням чого є недостатня дослідженість методів інформаційного впливу на конкретну особу [1, 10-15].

Важливим напрямом інформаційної безпеки в підприємницькій діяльності є протидія інформаційно-психологічному впливу. З розвитком ін-

формаційних технологій удосконалюються методи впливу за допомогою інформації на суспільство або окремих людей, технології маніпулювання поширюються на відносини у сфері підприємництва і значно випереджають розвиток способів та методів протидії такому впливу. Це може призвести до погіршення економічного становища та деградації суспільства.

Варто розуміти, що протидія інформаційно-психологічному впливу розглядається як один з інструментів інформаційного протиборства або вищої його стадії - інформаційної війни суб'єктів ринку. Тож в такому випадку інформаційний вплив здійснюється для нанесення збитків суб'єкту, до якого цей вплив застосовується. Як правило, захист підприємства реалізується через мінімізацію ризиків, проте такі заходи не завжди мають успішний результат. Тому потрібно застосовувати активну протидію інформаційно-психологічному впливу, а для цього також необхідно виділити об'єкти такої протидії. На підприємстві це, в першу чергу, працівники, з якими потрібно проводити заходи, які сприятимуть ліквідації негативних наслідків чужого інформаційно-психологічного впливу. Також об'єктом є інформаційне середовище, в якому розповсюджуються заходи інформаційно-психологічного впливу та сам суб'єкт, що зацікавлений в розповсюдженні такого впливу, а також суб'єкти, за допомогою яких розповсюджується такий вплив. Тож протидія повинна здійснюватися не з метою захисту, а задля припинення проведення інформаційно-психологічного впливу. Важливою формою заходів протидії є зрив та нейтралізація інформаційно-психологічного впливу, який здійснюється проти окремих підприємств.

У повсякденному житті людина користується певними моделями та готовими поглядами, що спрощує їй життя та допомагає швидше орієнтуватися в суспільстві. Тому під час проведення заходів інформаційно-психологічного впливу вагомим є створення таких моделей та доведення їх до конкретного об'єкта або виведення в інформаційний простір. Такі методи фактично мають характер програмування психіки окремих людей і суспільства в цілому. Для протидії негативному впливу також використовують стійкі моделі, які спрямовані на руйнування задумів інформаційно-психологічного впливу.

Залежно від об'єкта інформаційно-психологічного впливу на суб'єкт підприємницької діяльності різняться й методи його протидії. Якщо об'єктом виступає інформаційне середовище, то підприємству потрібно здійснювати заходи контрпропаганди, формування громадських об'єднань з клієнтів, акціонерів чи інших однодумців для поширення сформованих моделей протидії, також можуть влаштовуватися демонстрації, мітинги, пікети, а на додаток й поширення чуток та міфів, які руйнуватимуть технології негативного інформаційно-психологічного впливу. А в разі обрання суб'єктом впливу особи, яка ініціює чи проводить заходи такого впли-

ву, до неї застосовують інші методи протидії, такі як, наприклад, виявлення такої особи або осіб, через яких здійснюється такий вплив, викриття негативного змісту діяльності їх в інформаційному середовищі, звернення до органів влади або правоохоронних органів та інші.

Хоча здійснення заходів протидії інформаційно-психологічному впливу є новим для підрозділів безпеки підприємств, вони відповідно до своїх повноважень здатні до виконання функцій протидії інформаційно-психологічному впливу. Володіння ними необхідною інформацією для проведення певних заходів та опанування технологій протидії здатне забезпечити потрібні умови для реалізації їх під час інформаційної війни на ринку [2, 187-192].

Література

1. Абакумов В. М. Інформаційна безпека підприємництва як об'єкт адміністративно-правової охорони / В. М. Абакумов // Форум права. – 2012. – № 4. – С. 10-16 [Електронний ресурс]. – Режим доступу: http://arhive.nbuv.gov.ua/e-journals/FP/2012-4/12avmapo.pdf.

2. Інформаційна безпека в підприємницькій діяльності / М.І. Зубок. – К.: ГНОЗІС, 2015. – 216 с.

УДК 004.773

Люля В.С.
Огінська М.М.
Національна академія Служби безпеки України

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Сучасні інформаційні комунікації та соціальні мережі в їх числі стають ефективним інструментом суспільного розвитку і міждержавних відносин. Проте, їх зростаюча суспільна важливість зумовлює вразливість елементів інформаційної інфраструктури до негативних впливів. Інформаційна інфраструктура стала об'єктом інформаційної агресії, інформаційних воєн і постало питання: «Як забезпечити інформаційну безпеку?».

Сучасні соціальні мережі вщент заповнені гравцями-професіоналами. Їхньою функцією є вкидання «вибухової» інформації або розповсюдження дезінформації в більше чи менше коло користувачів соціальних мереж, подальша трансляція з їх допомогою максимально широкому загалу у вигляді сформованої серед певної частини населення громадської думки, настроїв і чуток. Не потрібно робити висновки , не перевіривши і не порівнюючи інформацію з офіційними джерелами.

Соціальні мережі збирають біографічні дані, щоб дозволити користувачам легко знаходити один одного. Така інформація також залучає мисливців за персональними даними. Перш ніж заповнювати анкету, подумайте трохи і певна частка скептицизму тут не завадить.

Існують ще так звані «боти»,головне завдання яких – керувати настроями людей у соцмережах. При цьому іноді ми навіть не здогадуємося, що ці коментарі в мережі могли бути написані взагалі неіснуючим користувачем. Фальшиві акаунти спеціалісти називають ботами (скорочення від «роботи»).

У дискусіях або конфліктних ситуаціях у соціальних мережах широко використовується прийом дзеркального повернення. Він передбачає спілкування з «опонентом» чи «групою опонентів» «їхньою мовою». Щоб схилити людину (чи спільноту в соціальній мережі) до своєї точки зору, маніпулятор передусім погоджується з думкою «опонента», причому «віддзеркалюючи» його манеру викладу. А потім пропонує власний варіант розвитку подій, який «опонентом» приймається вже як вірний.

З метою забезпечення інформаційної безпеки в соціальних мережах:

- Не варто розміщувати в Інтернеті персональну інформацію (номер мобільного телефону, домашню адресу та особисті фотографії).

- Не додавати незнайомих (або малознайомих) людей у власному аккаунті соцмереж, а також до контакт листа в профілях ICQ, Skype, Viber та в інших. Пам’ятати, що нові знайомі можуть бути не тими, за кого себе видають.

- Небажано відповідати на Спам, до якого відносяться листи щастя, пропаганда, DoS і DDoS-атаки, масова розсилка від імені іншої особи (для того щоб викликати до неї негативне ставлення), масова розсилка листів, що містять комп’ютерні віруси (для їх початкового поширення).

Забезпечення інформаційної безпеки в соціальних мережах – це складний процес , який потребує постійного контролю і вдосконалення. Не забезпечення інформаційної безпеки може послугувати для виникнення (корегування) певних уявлень, суджень, вчинків чи організації соціальних протестів, які використовуються внутрішніми і зовнішніми агресорами для вирішення різного роду цілей. Соціальні мережі можуть бути складовим елементом, як у локальних так і у військових конфліктах.

Література

1. Специфіка взаємодії в соціальних мережах. / Національна бібліотека України імені В. І. Вернадського / О. О. Лобовікова – [Електронний ресурс]. Режим доступу: http://www.irbisnbuv.gov.ua/cgibin/ irbis_nbuv/cgiirbis_64.exe? i21dbn=link&p21dbn=ujrn&z21id=&s21ref=10&s21cnr=20&s21stn=1&s21fmt=asp_meta &c21com=s&2_s21p03=fila=&2_s21str=stapttp_2014_62_22.

2. 4. Соціальні мережі, як середовище для технологій маніпулятивного впливу. / Сучасний захист інформації / Я. А. Деркаченко. – [Електронний ресурс]. Режим доступу: http://journals.dut.edu.ua/index.php/dataprotect/article/ view/531.

3. Як не стати жертвою в інформаційній війні. / Ракурс / О. Шклярська.– [Електронний ресурс]. – Режим доступу: http://ua.racurs.ua/520-informaciyna-viyna.

4. Боти у соцмережах: керувати суспільною думкою стає легше. / Uainfo правда із блогів / Є. Коляда. – [Електронний ресурс]. – Режим доступу: https://uainfo.org/blognews/1484641376-boti-u-sotsmerezhah-keruvati-suspilnoyu-dumkoyu-stae-legshe.html.

УДК 330.75

Ларіщев О.О.
Національна академія Служби безпеки України

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА

У сучасних умовах перед підприємствами та організаціями гостро постає завдання збереження як матеріальних цінностей, так і інформації, у тому числі відомостей, що становлять комерційну або державну таємницю.

Успіх виробничої і підприємницької діяльності в чималому ступені залежить від уміння розпоряджатися таким найціннішим товаром, як інформація, але вигідно використовувати можна лише ту інформацію, яка потрібна ринку. Тому в умовах посилення конкуренції успіх підприємництва, формується від надійної організації інформаційної безпеки підприємства.

Існує декілька визначень поняття «інформаційна безпека підприємства». Зокрема, Цимбалюк В. дає таке визначення - це суспільні відносини щодо створення та підтримання на належному (бажаному, можливому) рівні життєдіяльності відповідної інформаційної системи, у тому числі підприємництва [1].

Сороківська О. А. розглядає поняття «інформаційна безпека підприємства» як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб’єкта господарської діяльності [2].

Загрози інформаційної безпеки поділяються на внутрішні та зовнішні.

Зовнішні зловмисні дії можуть бути такими: копіюванні цінних документів, або викрадення файлів; викрадення флеш-карт; викрадення інформації у процесі її передавання по мережі Інтернет; пошкодження носіїв з інформацією; донесення інформації до фірм-конкурентів, або взагалі до іншої країни; викрадення інформації за допомогою інсайдерів; переманювання персоналу на іншу фірму.

До найбільш поширених внутрішніх загроз відносяться крадіжка, зараження інформації вірусами, або порча файлів службовцями компанії. До причин внутрішніх загроз відносяться: причини психологічного характеру у зв’язку з відносинами між співробітниками підприємства, що не склали-

ся; незадоволення рівнем заробітної плати; недобрі відносини між співробітником та керівництвом компанії [3].

Джерела загроз безпеці інформації підприємства можна розділити на три групи: антропогенні, техногенні та стихійні.

У групу антропогенних джерел загроз безпеки інформації входять: кримінальні структури, рецидивісти і потенційні злочинці; недобросовісні партнери і конкуренти; персонал установи (банку, його філій).

До техногенним джерелами загроз відносяться: неякісні технічні засоби обробки інформації; неякісні програмні засоби обробки інформації; засоби зв'язку, охорони, сигналізації; інші технічні засоби, що застосовуються в установі; глобальні техногенні загрози (небезпечні виробництва, мережі енерго-, водопостачання, каналізації, транспорт і т.п.).

До стихійним джерелами загроз відносяться пожежі, землетруси, повені, урагани та інші форс-мажорні обставини. Сюди ж входять і різні непередбачені обставини і нез'ясовні явища.

Відповідно до джерел загроз безпеці інформації підприємства визначаємо наступні напрями захисту інформації:

- Організаційно-технічне, в рамках якого створюється оболонка навколо об'єкта захисту, тобто інформаційних ресурсів, з певною мірою надійності виключає або суттєво утрудняє проведення маніпуляцій з інформацією в АС проти інтересів користувачів системи;

- Правове, спрямоване на створення імунітету, заснованого на загрозі застосування репресивного інструменту відносно порушників інтересів користувачів системи, і встановлює механізм застосування санкцій відносно правопорушника;

- Економічне, що передбачає механізм усунення матеріального збитку, завданого власнику інформації в результаті несанкціонованих дій з нею з боку правопорушника [4].

Отже, в умовах глобалізації забезпечення інформаційної безпеки на підприємстві полягає постійному контролі за джерелами виникнення потенційних загроз (антропогенні, технологічні та стихійні джерела) та необхідності здійснювати захист інформації різними способами (захист програм від читання та копіювання, захист авторських прав на інформацію, захист від несанкціонованого доступу і запуску програм, само тестування).

Література

1. Цимбалюк В. Інформаційна безпека підприємницької діяльності, визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації) //Підприємництво, господарство і право. – 2004. –№ 3. – С. 88-91.

2. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи [Текст] / О. А. Сороківська, В. Л. Гевко // Вісн. Хмельниц. нац. ун-ту. Сер.: Екон. науки. – 2010. – № 2. – Т. 2. – С. 32–35.

3. Танцюра М.Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим): автореф. дис.на здобуття наук ступеня канд. екон. наук: 08.00.04 / М.Ю. Танцюра. – Сімферополь, 2012. – 21 с.

4. Лук'яненко Д. Г. Стратегії глобального управління / Д. Г. Лук'яненко, Т. В. Кальченко // Міжнародна економічна політика. – 2009. – № 8-9. – С. 5-43.

УДК 342.9

Липний С.І.
Шепета О.В.
кандидат юридичних наук, доцент,
Національна академія Служби безпеки України

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Правову основу забезпечення захисту інформації в Україні як інституції права становлять Конституція України, закони України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про науково-технічну інформацію», інші нормативно-правові акти, в тому числі міжнародні договори України (які відповідним чином ратифіковані Україною), що стосуються сфери інформаційних відносин.

Державою розробляється і здійснюється державна інформаційна політика, що представляє собою систему правових, соціально-економічних, соціально-культурних і організаційних заходів.

Відповідно до ст. 3 Закону України «Про інформацію» головними напрямами державної інформаційної політики є: 1) забезпечення доступу кожного до інформації; 2) забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; 3) створення умов для формування в Україні інформаційного суспільства; 4) забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень; 5) створення інформаційних систем і мереж інформації, розвиток електронного урядування; 6) постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; 7) забезпечення інформаційної безпеки України; 8) сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору [1].

Інформаційну безпеку України можна визначити як стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства і держави.

Національне законодавство України надає великого значення інформаційній складовій національної безпеки. Так, норма ч. 1 ст. 17 Конституції України встановлює, що "захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу" [2]. У цьому контексті інформаційна безпека розглядається на одному рівні з такими невід'ємними атрибутами державності, як суверенітет і територіальна цілісність.

В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

Інформаційна війна, яку Росія активізувала з початком збройної агресії проти України, поставила перед нашою державою нові виклики у сфері інформаційної безпеки.

В Україні концептуальним документом щодо забезпечення інформаційної безпеки України та протидії російським інформаційним загрозам стала Доктрина інформаційної безпеки, ухвалена Радою національної безпеки та оборони у грудні 2016 р. і введена в дію Указом Президента П. Порошенка 25 лютого 2017р. [3].

Доктрина формалізує і закріплює на рівні нормативно правового акту факт агресії Російської Федерації проти України в інформаційній сфері, визначає основні загрози в інформаційній війні проти України, яка ведеться Російської Федерацією не тільки на території України, а в усьому світі. Відповідно в Доктрині зазначаються шляхи убезпечення і захисту: що саме треба удосконалити і зробити державі і її органам, щоб убезпечити суспільство від негативного інформаційного впливу інформаційної агресії Російської Федерації.

Аналіз положень Доктрини, зокрема розділу шостого, що визначає механізм реалізації Доктрини, показує, що Доктрина не збільшує втручання держави в реалізацію права на свободу слова і інформації більше, ніж це передбачено чинним законодавством України на даний момент. Декларація не вносить самостійно зміни до існуючого порядку, проте пропонує внести зміни в чинне законодавство з метою впровадження механізмів протидії агресії. Які саме це будуть зміни – у Доктрині прямо не зазначається, конкретних формулювань не міститься. Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни.

Очевидно, що запорукою створення надійної системи інформаційної безпеки сьогодні може бути тільки зміцнення самої української держави

та її державних органів, відповідальних за забезпечення інформаційної безпеки в країні. У зв'язку з цим стоять масштабні завдання, пов'язані з виробленням системи забезпечення інформаційної безпеки, пошуку принципово нових, нестандартних форм організації, взаємодії, координації діяльності, удосконалення всіх засобів, спрямованих на забезпечення процесу управління загрозами та небезпеками.

Література

1. Про інформацію: Закон України // База даних «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення 04.03.19).

2. Конституція України // База даних «Законодавство України/ ВР України. URL: https://zakon.rada.gov.ua/laws/main/254%D0%BA/96-%D0%B2%D1%80 (дата звернення 04.03.19).

3. Про рішення Ради національної безпеки і оборони України від 29.12.2016 «Про Доктрину інформаційної безпеки України» : Указ Президента України 25.02.2017 № 47/2017 // База даних «Законодавство України/ ВР України. URL: http://zakon2.rada.gov.ua/laws/show/47/2017(дата звернення 04.03.19).

УДК 351.862.4

Луцяк В.В.
Національна академія Служби безпеки України

ОСОБЛИВОСТІ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ В СУЧАСНИХ УМОВАХ

Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є дуже актуальними проблемами для нашої держави, яка часто є об'єктом зовнішньої інформаційної експансії, маніпулятивних пропагандистських технологій та руйнівного інформаційного вторгнення.

Увага до проблем гарантування інформаційної безпеки України зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, насильства, національної ворожнечі і є спробами руйнування національної ідентичності України, знищення міжнаціональної злагоди, посягання на конституційний лад України, територіальну цілісність держави. Проблема гарантування інформаційної безпеки України актуалізується в умовах війни на Сході України, коли з боку Російської Федерації відбувається інформаційна експансія, упереджене та тенденційне висвітлення фактів та явищ, а технології російських інформаційно-психологічних операцій спрямовані на забезпечення домінування в українському (а також у глобальному) інформаційному просторі та на утримання медійної переваги [1, с. 27-28].

Домінування на початку 2014 року в українському інформаційному просторі російських та проросійських ЗМІ та проведення спеціальних інформаційних операцій антиукраїнського характеру стали вирішальним чинником підготовки до анексії АР Крим та м. Севастополя, інспірування сепаратистських заворушень на Півдні та Сході України, що призвели врешті до тимчасової окупації окремих районів Донецької та Луганської областей, на території яких зараз триває операція об'єднаних сил (далі - ООС). За допомогою потужної пропагандистської кампанії під гаслами «русской весны» через телебачення, друковані ЗМІ, інтернет-видання та, передусім, соціальні мережі російські спецслужби намагалися здійснити масштабний вплив на свідомість громадян з метою інформаційного забезпечення створення так званої «Новоросії», дестабілізувати ситуацію у переважно російськомовних містах і регіонах України (Харкові, Одесі, Миколаєві, Херсоні та ін.) [2, с. 3]. Представник об'єднання "Інформаційний спротив" В.Гусаров виокремлює такі напрями інформаційно-психологічних атак проти України: 1) нав'язування думок про неспроможність української влади керувати державою та приймати раціональні рішення; 2) формування негативних суджень про воєнно-політичне керівництво України та про те, що хаотичні бойові дії призводять до невиправданих жертв серед сил ООС; 3) поширення поглядів про те, що українська армія на Сході України деморалізована та неспроможна вести бойові дії, а також про недовіру особового складу до керівництва; 4) нав'язування думки про те, що Україна не обійдеться без російського газу та що сторонам необхідно повернутися до перегляду газових контрактів. Експерт зазначає, що цільовою аудиторією Кремля зараз є населення РФ, російськомовна діаспора за кордоном, населення України, зокрема в окупованих районах Донбасу, громадяни західних країн, а також країн, близьких Росії за політичними поглядами [3].

Для вирішення проблем забезпечення інформаційної безпеки нашої держави постійно збирається та вивчається інформація щодо системних порушень прав людини та злочинів проти людяності на тимчасово окупованих територіях, серед іншого, переконливо спростовуються міфи російської пропаганди про начебто вимушений захист російсько-терористичними угрупуваннями населення цих територій від утисків з боку української влади. Послідовно займаються цією роботою волонтери, журналісти, правозахисні організації, активісти проекту «Стоп Терор», ГО «Безпека та взаємодія в Україні», ГО «Крим SOS», ГО «Донбас SOS» та інші громадські об'єднання. Долучаються до неї також зарубіжні та міжнародні неурядові аналітичні центри та правозахисні організації такі як: «Freedom House», «Amnesty International», «Репортери без кордонів» та ін. Так, наприклад, правозахисна організація «International Partnership for Human Rights» (IPHR) опублікувала звіт, у якому навела конкретні докази

незаконного перетину російсько-українського кордону збройними силами та військовою технікою РФ та обстрілів українських населених пунктів із російської території. Усі зібрані нею докази передаватимуться у міжнародні суди, що допоможе постраждалим від конфлікту захищати свої права та притягнути до відповідальності тих, хто віддавав злочинні накази [2, с. 16].

Отже, стратегічне інформаційне протистояння нині становить небезпечний компонент гібридної війни, розгорнутої Росією проти України, причому головною загрозою інформаційній безпеці нашої держави сьогодні залишається загроза впливу ворога на інформаційну інфраструктуру, інформаційні ресурси, на суспільство, свідомість і підсвідомість особистості з метою нав'язати власну систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності.

Література

1. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам/ У. Ільницька// Національний університет "Львівська політехніка". – 2016. – Політичні науки. Випуск № 1. Том 2. – С. 28-32. URL : http://ena.lp.edu.ua/bitstream/ntb/37314/1/7_31-36.pdf (дата звернення 06.03.2019).

2. Опалько Ю. В. Участь громадських об'єднань у протидії інформаційній агресії РФ/ Ю. В. Опалько// Національний інститут стратегічних досліджень. – Серія «Громадянське суспільство». Випуск № 14. – С. 25. URL : http://www.niss.gov.ua/content/articles/files/AZ-Protid-ya--nformagres---166e3.pdf (дата звернення 06.03.2019).

3. Гусаров В. Кремль розпочав нову інформаційну операцію проти України / В. Гусаров. URL : http://www.osvita. mediasapiens.ua/material/34281 (дата звернення 06.03.2019).

УДК 004.492

Максименко А.А.
Козюра В.Д.
кандидат технічних наук, доцент,
Національна академія Служби безпеки України

ПРОГРАМНІ ЗАКЛАДКИ ТА МЕТОДИ ЗАХИСТУ КОМП'ЮТЕРНИХ СИСТЕМ ВІД НИХ

Програмні закладки, впроваджені в програмне забезпечення інформаційно-телекомунікаційних систем, використовуваних на об'єктах критичної інфраструктури держави, представляють серйозну загрозу для національної безпеки України.

Неформально програмну закладку можна визначити як програму (фрагмент коду програми), яка приховано впроваджена в систему, що ата-

кується, і дозволяє користувачеві, що знає про її присутність, здійснювати несанкціонований доступ до тих чи інших ресурсів системи [1]. На відміну від шкідливих програм, поширення яких, як правило, не носить цілеспрямованого характеру, а здійснюється фронтально, програмні закладки використовують проти конкретних систем, як засіб таргетованих атак.

Програмні закладки класифікуються:

1) За методом впровадження в комп'ютерну систему:

- програмно-апаратні закладки, які асоційовані з апаратними засобами (їх місцем існування є BIOS, відео- і мережеві карти);
- завантажувальні закладки, які асоційовані з програмами, що розташовуються в завантажувальних секторах жорсткого диска;
- драйверні закладки, які асоційовані з драйверами периферійних пристроїв персонального комп'ютера;
- закладки-імітатори, що імітують інтерфейс службових програм, виконання яких передбачає введення конфіденційної інформації;
- замасковані закладки, що маскуються під програми, що дозволяють оптимізувати роботу персонального комп'ютера, комп'ютерні ігри та інші розважальні програми [2, 3].

2) За основними діям деструктивного характеру, які здійснюються за допомогою комп'ютерної системи:

- закладки, які здійснюють копіювання конфіденційної інформації користувачів, яка знаходиться в оперативній пам'яті, зовнішньої пам'яті системи, або в пам'яті іншої системи, підключеної по локальної або глобальної мережі;
- закладки, які здійснюють зміну алгоритмів функціонування системних, прикладних та службових програм;
- закладки, які здійснюють зміну режимів роботи програмного забезпечення [2].

Наявні на даний момент методи захисту комп'ютерних систем від програмних закладок можна розділити на дві групи:

1) методи застосування штатних захисних засобів комп'ютерної системи для побудови і підтримки політики безпеки, адекватної щодо захисту від програмних закладок;

2) методи застосування спеціалізованих програмних засобів, призначених для виявлення, попередження та припинення дозволяють впливів на комп'ютерну систему з боку програмних закладок [1, 3].

Існують наступні методи захисту :

- сканування системи на предмет наявності відомих програмних закладок – даний метод полягає в тому, що система протидії програмним закладкам час від часу здійснює сканування фізичних накопичувачів комп'ютера на предмет наявності програмних закладок;

- контроль цілісності програмного забезпечення – метод полягає в тому, що для кожного програмного модуля, що присутній в системі, що захищається, заздалегідь підраховуються довжина і контрольна сума (ця інформація зберігається в файлі, підписаному цифровим підписом);
- контроль цілісності конфігурації системи, що захищається, – метод полягає в тому, що для усіх елементів конфігурації системи, які можуть бути змінені при впровадженні в систему програмної закладки, створюються еталонні копії (надалі регулярно проводиться порівняння цих елементів конфігурації з їх еталонними копіями);
- моніторинг інформаційних потоків – будь-яка програмна закладка втручається в інформаційні потоки, які відбуваються всередині комп'ютерної системи, в яку вона впроваджена;
- програмні пастки – метод полягає в створенні в системі, що захищається, «привабливих» для порушників об'єктів, доступ до яких неможливий без використання програмних закладок. Усі успішні звернення до таких об'єктів реєструються [1].

Висновки. Основна небезпека програмних закладок полягає в тому, що закладка здатна приймати активні заходи щодо маскування своєї присутності в системі. Програмні закладки виконують роль перехоплювачів паролів, трафіку, а також служать в якості провідників для створення таргетованих атак на об'єкти критичної інфраструктури.

Література

1. Проскурин В.Г. Защита программ и данных: учеб, пособие для студ. учреждений высш. проф. образования / В.Г.Проскурин. 2-е изд., стер. - М.: Издательский центр «Академия», 2012. – 208 с.

2. Программная закладка. [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Программная_закладка.

3. Макнамара Д. Секреты компьютерного шпионажа: Тактика и контрмеры / Д. Макнамара; Пер. с англ.; Под ред. С.М.Молявко. – М.: БИНОМ. Лаборатория знаний, 2004. – 536 с.

УДК 351.862.4

Міщенко І.С.
Національна академія Служби безпеки України

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ ВІД ДЕСТРУКТИВНОГО ВПЛИВУ ДЕРЖАВИ-АГРЕСОРА

Відповідно до положень Стратегії національної безпеки України однією з актуальних загроз національній безпеці є інформаційно-психологічна

війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу [1].

Специфіка гібридної війни визначає інформацію як один із ключових засобів масового ураження. По суті, інформаційний простір поступово перетворюється на окрему, поряд із традиційними "земля", "повітря", "море", сферу ведення бойових дій, у якій все більш активно діють відповідні підрозділи збройних сил Російської Федерації, представники яких нещодавно визнали, що мають у своїй структурі війська інформаційних операцій. У зв'язку із вищевикладеним особливої актуальності набуває забезпечення інформаційної безпеки (захищеності свідомості людини та масової свідомості від негативного інформаційного впливу) та безпеки інформації (стану, що забезпечує захист інформації від загроз для неї) [2].

Специфіка інформаційної війни зумовлює ряд особливостей, які кардинально відрізняють її від традиційних військових дій:

1. Об'єктом інформаційного впливу є не лише противник, а й громадяни власної країни. Потужна пропагандистська машина РФ активно працює на консолідацію населення проти українців, викривляючи події історії та сучасні новини. Крім того, так звані «фейки» використовуються як джерело легітимізації агресії на Сході України, окупації Автономної Республіки Крим та незаконних рішень вищого керівництва країни.

2. Не існує чіткого локально визначеного місця ведення бойових дій. Інформаційний влив здійснюється на усіх можливих платформах одночасно. Основними театрами бойових дій є телебачення, друковані ЗМІ, Інтернет, соціальні мережі.

3. Відсутність очевидних втрат, зокрема, фізичних, внаслідок ведення інформаційної війни. Проте реальні наслідки згодом відчуваються під час проведення «традиційних» бойових операцій. Наслідки поразки в інформаційній війні Україні доводиться долати вже п'ятий рік поспіль [3].

З метою запобігання проведенню спеціальних інформаційних операцій та мінімізації негативних наслідків виникає необхідність вжиття відповідних заходів. Основними суб'єктами протидії інформаційному впливу є уповноважені державні органи, підрозділи правоохоронних органів, представники ЗМІ та активна громадськість.

Міжнародне співробітництво з іноземними державами та компаніями протягом останніх років набуває особливого розвитку та має відповідні результати. Зокрема, соціальна мережа Фейсбук за заявами України регулярно блокує акаунти антиукраїнського спрямування. Європейські держави виступають активними партнерами під час планування заходів з протидії інформаційному впливу РФ, допомагають у створенні координаційних центрів протидії спеціальним інформаційним операціям та беруть активну

участь у підвищенні кваліфікації працівників правоохоронних органів та вдосконаленні матеріально-технічної бази уповноважених державних органів [4].

Також актуальним в умовах сьогодення є створення інформаційних ресурсів типу «Стоп Фейк», метою яких є моніторинг російських ЗМІ та спростування неправдивих і викривлених повідомлень та новин. Зауважимо, що вказаний ресурс функціонує декількома європейськими мовами, щоб громадяни країн-партнерів також були проінформовані про підступні випадки викривлення фактів збоку Російської Федерації. Проте досить невисока популярність подібних ресурсів не дозволяє повною мірою реалізувати її переваги та донести їхній зміст до громадськості. Випуски подібних програм охоплюють аудиторію біля 2 тис осіб в інтернет-сервісі Youtube. Виходячи з цього, очевидною є необхідність популяризації таких ресурсів для забезпечення їх максимальної ефективності [5].

Отже, Україна вживає активних заходів щодо протидії інформаційним загрозам та поступово нарощує свої сили на інформаційному фронті війни з Росією. Органи державної влади потребують постійного удосконалення відповідного технічного забезпечення, а уповноважені посадові особи — рівня своєї компетенції, на що сьогодні спрямовані великі зусилля держави. Підтримка громадян України, їх проінформованість та правильне розуміння і оцінка подій – одна із основних складових забезпечення національної безпеки.

Література

1. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України». URL: http://zakon5.rada.gov.ua/laws/show/287/2015 (дата звернення 06.03.2019).

2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». URL : http://zakon2.rada.gov.ua/laws/show/96/2016 (дата звернення 06.03.2019).

3. Що таке інформаційна війна. URL: http://my.elvisti.com/sergandr/iv.html(дата звернення 06.03.2019).

4. Facebook News room. Removing Coordinated Inauthentic Behavior from Russia. URL:https://newsroom.fb.com/news/2019/01/removing-cib-from-russia (дата звернення 06.03.2019).

5. Stop Fake определил российскую дезинформацию как главную угрозу в глобальной повестке.URL: https://www.stopfake.org/yakub-yanda-stopfake-opredelil-rossijskuyu-dezinformatsiyu-kak-glavnuyu-ugrozu-v-globalnoj-povestke (дата звернення 06.03.2019).

УДК 316.485
Монастирна Л.О.
Скубко О.П.
Національна академія Служби безпеки України

МАНІПУЛЯТИВНІ ТЕХНОЛОГІЇ ВПЛИВУ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ НА НАСЕЛЕННЯ УКРАЇНИ ЧЕРЕЗ ЗАСОБИ МАСОВОЇ ІНФОРМАЦІЇ

РФ веде активну гібридну війну проти України, в тому числі, через інформаційно-телекомунікаційні системи, засоби інформування, інформаційні ресурси тощо, оскільки населення України має вільний доступ до будь-яких джерел, у тому числі, які містять неперевірену і недостовірну інформацію.

Аналізуючи інформацію в ЗМІ, виступах політичних еліт РФ на телеканалах, Інтернет - джерелах можна навести ряд основних напрямів застосування РФ маніпулятивних технологій:

- спотворення історичних подій;
- формування стереотипу меншовартості та вторинності на тлі непереможності армії РФ;
- удари по іміджу України на міжнародній арені з метою послаблення геополітичного значення нашої держави;
- дезінформація населення через ЗМІ задля посилення дестабілізації емоційного стану населення та впровадження хаосу серед населення, витіснення української мови, поширення російської культури та традицій як основних джерел самоідентифікації нації.

Російська Федерація здійснює інформаційно-психологічний вплив різноманітними способами: друкованими періодичними виданнями, книговиданням, через телебачення, радіо, Інтернет та інші спеціальні засоби.

Розкриваючи способи та основні напрями застосування маніпулятивних технологій щодо формування негативного іміджу України на міжнародній арені засобами телебачення, ми проаналізували телевізійні матеріали України та світового співтовариства.

Російське телебачення в своїх новинах багато говорить про події в Україні, але дуже мало часу приділяє тому, що відбувається в Росії. Таких висновків дійшла робоча група Євросоюзу з подолання дезінформації.

Аналітики переглядали передачі на російському телебаченні впродовж 13-19 жовтня та підсумували, що 71 теми, 60 було про події поза Росією. Дослідники також порахували вагу повідомлень про світ поза РФ в 15 політичних та аналітичних ток-шоу на трьох найбільш популярних в РФ каналах: "Первый", "Россия – 1" та "НТВ", пише "Голос Америки" [1].

При цьому у кожному випуску програм фігурує Україна, трохи рідше США та ЄС. Водночас теми, що стосуються Росії в окремих випусках можуть не підніматись взагалі.

Нині в Україні зареєстровано приблизно 791 телевізійну організацію (513 приватних, 29 державних). Більшість приватних телекомпаній в регіонах України, створених не без сприяння російського капіталу, ведуть передачі, як правило, російською мовою. Ні регіональні, ні центральні телекомпанії, які отримали ліцензії на роботу в українському телеефірі, не дотримуються вимоги закону, яка передбачає, що не менше половини телепродукції має виготовлятись в Україні. Деякі компанії спеціалізуються на ретрансляції передач російського телебачення. Державний комітет телебачення і радіомовлення України визнав, що "типовою ознакою телерадіопростору України є засилля іноземної продукції, легковажні, сумнівної якості програми"[2].

Російські ЗМІ висвітлюють події в Україні тенденційно, не особливо приховуючи свої "імперські" настрої із застосуванням методів дозування інформації, викривлення ходу подій, дезінформацію, інформаційний сурогат, вибіркову подачу матеріалу, інформаційний рефреймінг (підбираючи відповідний контекст до і після трансляції повідомлення, а також під час повідомлення - у вигляді коментарів). Застосовуються також методи подачі інформації "без коментарів" після налаштування необхідних фільтрів сприйняття у слухача попередніми повідомленнями, перебільшення і замовчування інформації.

Отже, можна стверджувати те, що на сьогоднішній день Російська Федерація здійснює інформаційний вплив на власне, українське населення, а також на світове співтовариство задля навіювання власної точки зору щодо сьогоднішньої геополітичної реальності.

Література

1. Російське телебачення найчастіше говорить про Україну та США//Дзеркало тижня, 24 жовтня, 2017. – [Електронний ресурс]. – Режим доступу: https://dt.ua/WORLD/rosiyske-telebachennya-naychastishe-govorit-pro-ukrayinu-ta-ssha-257956_.html.

2. Багато про Україну і нічого про Росію: в ЄС зробили огляд російського телебачення//УНІАН, 24 жовтня, 2017. – [Електронний ресурс]. – Режим доступу:https://www.unian.ua/world/2205199-bagato-pro-ukrajinu-i-nichogo-pro-rosiyu-v-es-zrobili-oglyad-rosiyskogo-telebachennya.html.

УДК 621.391.
Пахольченко В.О.
Гордієнко С.Б.
кандидат технічних наук, доцент,
Національна академія Служби безпеки України

АКТУАЛЬНІ ПИТАННЯ ІНФРАСТРУКТУРИ КІБЕРПРОСТОРУ ЩОДО МЕРЕЖНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Мережна технологія – це погоджений набір стандартних протоколів та програмно-апаратних засобів, які їх реалізовують в обсязі, достатньому для побудови локальної обчислювальної мережі. Це визначає, як буде отримано доступ до середовища передачі даних [1]. В якості альтернативи можна ще зустріти назву «базові технології».

Передумови створення

Створення комп'ютерних мереж було обумовлено прагненням до економії ресурсів. Економія досягається кількома шляхами:

1. мережа забезпечує швидкий доступ до різних джерел інформації;
2. мережа зменшує надмірність ресурсів.

Комп'ютерна мережа забезпечує:

1. колективне опрацювання даних користувачами, комп'ютери яких під'єднані до мережі, та обмін даними між цими користувачами;
2. спільне використання програм;
3. спільне використання принтерів, модемів та інших периферійних пристроїв.

Ethernet: На даний момент це сама популярна у всьому світі мережева технологія. У розвиток мережної технології Ethernet створені високошвидкісні варіанти: ***Ieee802.3u/Fast Ethernet*** *і* ***Ieee802.3z/Gigabit Ethern*****et**. Основна топологія, яка використовується в локальних мережах Fast Ethernet і Gigabit Ethernet – *пасивна зірка*.

1. Мережна технологія Fast Ethernet забезпечує швидкість передачі 100 Мбіт/с.
2. Мережна технологія локальних мереж Gigabit Ethernet – забезпечує швидкість передачі 1000 Мбіт/с.

Локальні мережі Fast Ethernet і Gigabit Ethernet сумісні з локальними мережами, виконаними за технологією (стандарту) Ethernet, тому легко і просто сполучати сегменти Ethernet, Fast Ethernet і Gigabit Ethernet в єдину обчислювальну мережу.

Token-Ring: Мережні інформаційні технології даного типу використовуються для створення розділеного середовища передачі даних, яка в кінцевому підсумку утворюється як об'єднання всіх вузлів в одне кільце.

Будується дана технологія на зірково-кільцевій топології. Перша йде як основна, а друга - додаткова. Щоб отримати доступ до мережі, застосовується маркерний метод. Максимальна довжина кільця може становити 4 тисячі метрів, а кількість вузлів - 260 штук. Швидкість передачі даних при цьому не перевищує 16 Мбіт/секунду.

ArcNet Цей варіант використовує топологію шина і пасивна зірка. При цьому він може будуватися на неекранованій витій парі та оптоволоконному кабелі.

ArcNet - це справжній старожил у світі мережних технологій. Довжина мережі може досягати 6000 метрів, а максимальна кількість абонентів - 255. При цьому слід зазначити основний недолік цього підходу - його низьку швидкість передачі даних, яка становить тільки 25 Мбіт/с. Але ця мережна технологія все ще широко використовується. Це відбувається завдяки її високій надійності, низькій вартості адаптерів і гнучкості. Мережі і мережні технології, побудовані за іншими принципами, можливо, і володіють більш високими показниками швидкості, але саме з-за того, що ArcNet забезпечує високу поставку даних, це дозволяє нам не скидати її з рахунків. Важливою перевагою даного варіанту є те, що використовується метод доступу за допомогою передачі повноважень [1].

FDDI: Мережні комп'ютерні технології даного виду є стандартизованими специфікаціями архітектури високошвидкісної передачі даних, що використовує оптоволоконні лінії. На FDDI значним чином вплинули ArcNet і Token-Ring. Тому цю мережну технологію можна розглядати як вдосконалений механізм передачі даних на підставі наявних напрацювань. Кільце цієї мережі може досягати в довжину сто кілометрів. Незважаючи на значну відстань, максимальна кількість абонентів, які можуть підключитися до неї, становить лише 500 вузлів. Слід зазначити, що FDDI вважається високонадійною завдяки наявності основного та резервного шляхів передачі даних. Додає їй популярність і можливість швидко передавати дані - приблизно 100 Мбіт/с.

Є ЕОМ, які об'єднані в одну мережу. Умовно вони поділяються на абонентські (основні) і допоміжні. Перші займаються всіма інформаційно-обчислювальними роботами. Від них же залежить те, якими будуть ресурси мережі. Допоміжні займаються перетворенням інформації та її передачі по каналах зв'язку. Із-за того, що їм доводиться обробляти значну кількість даних, сервери можуть похвалитися підвищеною потужністю. Але кінцевим одержувачем будь-якої інформації все ж є звичайні хост-ЕОМ, які найчастіше представлені персональними комп'ютерами [1]. Мережні інформаційні технології можуть використовувати такі типи серверів:

1. *Мережевий.* Займається передачею інформації.
2. *Термінальний*. Забезпечує функціонування багатокористувацької системи.

3. *Баз даних*. Займається обробкою запитів до БД в багатокористувацьких системах.

Мережі з комутацією каналів. Вони створюються завдяки фізичному з'єднанню клієнтів на той час, коли будуть передаватися повідомлення. У таких випадках для відправки і отримання інформації від точки А до точки Б створюється пряме з'єднання. Воно включає в себе канали одного з безлічі (як правило) варіантів доставки повідомлення. І створене з'єднання для успішної передачі повинно бути незмінним протягом усього сеансу. Але в такому випадку виявляються досить сильні недоліки. Так, доводиться довго чекати з'єднання. Це супроводжується високою вартістю передачі даних і низьким коефіцієнтом використання каналу. Тому використання мережних технологій даного типу не поширене.

Мережі з комутацією повідомлень. У цьому випадку вся інформація передається невеликими порціями. Пряме з'єднання в таких випадках не встановлюється. Передача даних здійснюється по першому ж вільному з доступних каналів. І так до тих пір, поки повідомлення не буде передано своєму адресату. Сервера при цьому постійно займаються прийомом інформації, її збиранням, перевіркою і встановленням маршруту [2]. З переваг необхідно відзначити низьку ціну передачі. Але в такому разі все ще існують такі проблеми, як низька швидкість і неможливість здійснення діалогу між ЕОМ в режимі реального часу.

Мережі з комутацією пакетів. Це найдосконаліший і популярний на сьогодні спосіб комутації. Розвиток мережних технологій призвів до того, що зараз обмін інформацією здійснюється за допомогою коротких пакетів інформації фіксованої структури. Пакети – це частини повідомлень, що відповідають певному стандарту [2]. Невелика їх довжина дозволяє запобігти блокування мережі. Завдяки цьому зменшується черга у вузлах комутації. Здійснюється швидке з'єднання, підтримується невисокий рівень помилок, а також досягнуті значні результати в плані збільшення надійності і ефективності мережі. Слід зазначити і те, що існують різні конфігурації цього підходу до побудови. Так, якщо мережа забезпечує комутацію повідомлень, пакетів і каналів, то вона називається інтегральною, тобто можна провести її декомпозицію. При використанні пакетної технології важливим є налагодження та узгодження великої кількості клієнтів, ліній зв'язку, серверів і цілого ряду інших пристроїв. В цьому допомагає встановлення правил, які відомі як протоколи. Вони є частиною використовуваної мережної операційної системи і реалізуються на апаратному та програмному рівнях.

Література

1. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. – Львів: «Магнолія 2006», 2013. – 256 с. ISBN 978-617-574-087-3.

2. Буров Є. В. Комп'ютерні мережі: підручник / Євген Вікторович Буров. – Львів: «Магнолія 2006», 2010. – 262 с. ISBN 966-8340-69-8.

УДК 351.75
Петняк В.В.
Тиква В.Л.
Національна академія Служби безпеки України

РОЗВІДУВАЛЬНІ ПРОГРАМИ СПЕЦСЛУЖБ США ЯК ІНСТРУМЕНТ БОРОТЬБИ З ЕКСТРЕМІЗМОМ

Загальноприйнятою є думка, що існування високотехнологічного обладнання систем розвідувальних органів, яке надає урядовим структурам доступ до особистої інформації громадян на кшталт прослуховування телефонних розмов або спілкування за допомогою електронної пошти, суперечать конституційним нормам, особливо в частині, про право кожної людини на приватне життя. Проте, такі системи існують у багатьох розвинених країнах світу.

Сьогодні екстремістські рухи набули міжнародного, глобального характеру і є реальною та серйозною загрозою національній та міжнародній безпеці, мають тенденцію до зростання, що засвідчує загальна кількість екстремістських акцій і число країн, в яких вони відбуваються [1].

Сучасний характер екстремізму, збільшення його масштабів у світі, застосування жорстоких, а інколи й підступнихформ в процесі проведення несанкціонованих протестнихакцій викликає велике занепокоєння у світі. В офіційних документах ЄС, ООН, низці міжнародних договорів та угод екстремізм характеризується як загроза стратегічного рівня.

Незважаючи на заходи, які запроваджуються окремими державами і світовим співтовариством у цілому, в XXI столітті, навряд чи варто чекати остаточної ліквідації тероризму. Більше того, є всі підстави вважати, що екстремізм може стати ще поширенішим та більш згуртованим. І трагічні події 11 вересня 2001 року в США -цьому підтвердження.

Саме після терактів 11 вересня Уряд США таємно дозволив АНБ підключатися до оптоволоконних кабелів, які входять і виходять із США, знаючи, що це дасть несанкціонований доступ до приватного життя американців. Моніторинг комунікацій дає АНБ доступ до електронної пошти, телефонних дзвінків, відеочатів, вебсайтів, фінансових транзакцій тощо [1].

Для здійснення задуманого, у 2007 році АНБ США створило програму PRISM, що здатна брати велику кількість потоків інформації і допомагати уряду створити з них дискретний керований потік даних.

PRISM - секретна програма електронного спостереження та збору розвідувальної інформації у веденні Агентства національної безпеки США, яка здатна збирати два види інформації: дані та метадані. Метадані – це побічний продукт комунікацій, як приклад: записи телефонних роз-

мов, час та тривалість дзвінка, паролі до електронних скриньок, IP-адреси та пошукові історії браузерів.

Інформація, яка колекціонується PRISM включає дані про зміст електронних листів, чатів, голосових дзвінків, збережених файлів на хмарних сховищах тощо. Усе це, допомагає спеціалістам з АНБ виявити та запобігти вчиненню масштабних акцій екстремістської та терористичної спрямованості.

Програма PRISM обслуговується підрозділами АНБ, які в кращих традиціях розвідувальної спільноти США співпрацюють з-понад 100 дочірніх американських компаній.

Обслуговування програми PRISM становить близько 20 млрд дол. у рік. ФБР виступає в якості посередника між розвідувальними агентствами і технологічними компаніями у запуску і функціонування програми. Сама програма тотальна, оскільки в ній фігурує і такий найбільший виробник комп'ютерної техніки, як корпорація Dell[2].

Крім того, PRISM здійснює збір та аналіз інформації отриманих від таких потужних компаній як: Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, AOL, Skype та Apple. Едвард Сноуден, колишній співробітник АНБ США зазначає, що 98% оброблюваної PRISM інформації, надходять від YAHOO, Google та Microsoft.

PRISM - система, що дозволяє майже в автоматичному режимі збирати і зберігати гігантські потоки цифрових даних. Їй не потрібен дозвіл для цього, оскільки вона пропускає через себе майже весь трафік, як приклад, не кожна компанія буде зберігати повідомлення в месенджерах, записи відеоконференцій або історію чату. Але PRISM завдяки своїм технологіям збору метаданих може надати копії всього вищеназваного зі своїх архівів.

Як зазначає WashingtonPost, існує ще як мінімум три урядові програми, подібні PRISM, над якими також опікується АНБ: MAINWAY, MARINA і NUCLEON. Разом програми охоплюють величезні території, збираючи метадані телекомунікацій та інтернет-потоку, що проходять через США[3].

Разом з тим, чимало експертів занепокоєнні та вбачають загрозу у PRISM, адже система здатна шпигувати не лише за потенційними чи реальними екстремістами й терористами, а й здійснювати тотальний контроль над власним громадянами. Світові ЗМІ зазначають, що програми на кшталт PRISM ставлять хрест на свободі інформації в інтернеті та недоторканності приватного життя.

Глибоко в океані проходить більша частина світових телекомунікацій та інтернет-трафіку. З 1970-х років АНБ дали можливість впроваджуватися в потоки даних, що проходять через ці кабельні системи. І їм не потрібен дозвіл. Щодо інтернету, то межі тут не мають значення. Якщо ви по-

силаєте лист з однієї країни до іншої, то цілком може статися, що дані пройдуть через ті ж сервери, розташовані на території США [4].

Питання щодо існування подібних до PRISM розвідувальних систем, що здатна щодня перехоплювати близько 1.7 млрд. розмов, повідомлень та розмов не є однозначним. Існування таких систем гостро порушує питання щодо права кожного громадянина на приватне спілкування та життя, яке закріплюється конституційними нормами. З іншого боку, потрібно розуміти, що забезпечення державної та національної безпеки держави, потребує подібні жертви. А втім, на сьогоднішній день, не існує технічних обмежень, які б змогли завадити спеціальним службам отримати доступ до будь-якої телефонної розмови чи повідомлення [5].

Література

1. Резнікова О.О. Актуальні питання протидії тероризму у світі [Електронний ресурс] / Резнікова О.О. – 2017. – Режим доступу до ресурсу: http://www.niss.gov.ua/content/articles/files/aktualniPitannya_press-1c1ef.pdf.

2. PRISM - лише одна з систем стеження [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://dt.ua/WORLD/zahidni-zmi-perekonani-scho-prism-lishe-odna-z-sistem-stezhennya-123720_.html.

3. Here’severything weknowabout PRISM todate [Електронний ресурс] // The Washington Post. – 2013. – Режим доступу до ресурсу: https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/?noredirect=on&utm_term=.270a38f054e1.

4. NSA Prismprogram tapsintouser data of Apple, Googleandothers [Електронний ресурс] // The Guardian. – 2013. – Режим доступу до ресурсу: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

5. PRISM [Електронний ресурс] // Security Lab. – 2015. – Режим доступу до ресурсу: https://www.securitylab.ru/news/tags/PRISM/.

УДК 343.13

Писарчук Р.В.
Національна академія Служби безпеки України

ДО ПРОБЛЕМИ УТОЧНЕННЯ ПОНЯТТЯ «ПРИВАТНЕ СПІЛКУВАННЯ»

У загальному розумінні «поняття», це форма мислення, що відбиває предмети у їх істотних ознаках. Правильно сформульоване поняття розкриває зміст явища, предмета, дії тощо. Зважаючи на це, становлення та розвиток будь-якої науки забезпечується стабільним понятійним апаратом, що своєю чергою є надійним інструментом розробки відповідної теорії та узагальнення практики існування досліджуваного явища чи процесу. Не винятком у контексті зазначеного є і «втручання у приватне спілкуван-

ня», стан розвитку наукових знань щодо якого у науці кримінального процесу бере свій початок ще у минулому столітті. Втім, його правильне визначення чи уточнення навряд чи можливе без визначення такого поняття, як «приватне спілкування».

Сучасне життя суспільства наповнене постійним спілкуванням. Усно та письмово люди спілкуються особисто, за телефоном, у соціальних мережах тощо. Життя соціально активної особи взагалі представляє собою майже безперестанне спілкування, зважаючи на що його роль у приватному житті, громадській чи професійній діяльності надзвичайно велика. Досить часто спілкування розглядається як певний вид діяльності, один із елементів загальної культури людства. Враховуючи, що спілкування пронизує усі сфери суспільного життя, воно вивчається численними науками (філологія, філософія, психологія, юриспруденція тощо), у кожній із яких вчені підходить до цього феномену зі своїх позицій.

Так, Великий тлумачний словник сучасної української мови визначає «спілкування» як «взаємні стосунки»; «діловий, дружній зв'язок»; «передача інформації однією особою іншій» [1, с. 1368].

У Філософському словнику соціальних термінів спілкування розглядається як одна із основних форм людської взаємодії, істотна ознака життєдіяльності особистості, як суспільної істоти, основу якого становить спільна предметна, насамперед виробнича діяльність, потреба у взаємодопомозі та взаєморозумінні [2, с. 556-557].

Варто також звернути увагу на функції спілкування, які у психології, залежно від його мети, поділяються на такі види: 1) контактна, мета якої – установлення контакту як стану обопільної готовності до приймання і передачі повідомлень та підтримання взаємозв'язку; 2) інформаційна – обмін повідомленнями, думками, задумами, рішеннями тощо; 3) спонукальна – стимуляція активності партнера для спрямування його на виконання певних дій; 4) координаційна – взаємне орієнтування й узгодження дій при організації спільної діяльності; 5) розуміння – не лише адекватне сприйняття змісту повідомлення, а і взаєморозуміння намірів, установок, переживань, станів тощо; 6) емоційна – збудження в партнері потрібних емоційних переживань, обмін ними, а також зміна з його допомогою власних переживань і станів; 7) установлення відносин – усвідомлення й фіксація свого місця в системі рольових, статусних, ділових, міжособистісних та інших зв'язків співтовариства, у якому діє індивід; 8) впливу – зміна стану, поведінки, індивідуально-смислових утворень партнера, у тому числі його намірів, установок, думок, рішень, уявлень, потреб, дій чи активності [3, с. 511-512].

У сфері кримінальної процесуальної діяльності, згідно ч. 3 ст. 258 КПК України, спілкування визначається як передавання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою

засобів зв'язку будь-якого типу. Спілкування є приватним, якщо інформація передається та зберігається за таких фізичних чи юридичних умов, при яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб [4].

Коментуючи зазначене визначення вчені-процесуалісти зауважують, що спілкування слід вважати приватним лише тоді, коли його учасники застосовують необхідні запобіжні заходи, які, на їх думку, перешкоджають розповсюдженню обмінюваної інформації [5, с. 657]. За таких обставин вживання словосполучення «можуть розраховувати на захист інформації від втручання» є досить дискусійним, оскільки за відповідних умов особа повинна мати «достатні підстави так вважати», бути «впевненою», а не «розраховувати» на захист від свавільного втручання в приватне спілкування. До речі, у ч. 4 ст. 258 КПК України, у контексті втручання в приватне спілкування, вжито саме словосполучення «достатні підстави вважати», а не «можуть розраховувати», що таке спілкування є приватним [4].

Зважаючи на викладене, пропонуємо уточнити термін «приватне спілкування», виклавши його у такій науковій редакції: *приватне спілкування – це передавання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв'язку будь-якого типу за таких фізичних і юридичних умов, при яких учасники спілкування мають достатні підстави вважати, що вона захищена від свавільного втручання інших осіб.*

Потреба у визначенні цього поняття зумовлена тим, що його чітка інтерпретація має важливе значення для визначення і осмислення значення терміну «втручання в приватне спілкування» та суміжних з ними понять, що вживаються у законодавстві.

Література

1. Великий тлумачний словник сучасної української мови / авт. кол.; уклад. і гол. ред. В.Т. Бусел. Ірпінь: ВТФ «Перун», 2009, 1736 с.

2. Філософський словник соціальних термінів / авт. кол. Харків: Корвін, 2002, 672 с.

3. Психологічний тлумачний словник найсучасніших термінів / авт. кол. Харків: Прапор, 2009. 672 с.

4. Кримінальний процесуальний кодекс України // *Відомості Верховної Ради України*. 2013. № 9-10, 11-12, 13. Ст. 88.

5. Кримінальний процесуальний кодекс України. Наук.-практ. коментар: у 2 т. / О.М. Бандурка, Є.М. Блажівський, Є.П. Бурдоль та ін.; за заг. ред. В.Я. Тація, В.П. Пшонки, А.В. Портнова. Харків: Право, 2012. Т. 1. 768. Т. 2. 664 с.

УДК 354.42/.44:340.134(477)
Поліщук О.В.
Требко А.О.
Національна академія Служби безпеки України

АКТУАЛЬНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Складна політична ситуація, в якій знаходиться Україна останні роки, гібридна війна з Росією і постійне погіршення іміджу держави в міжнародному співтоваристві обумовлені низкою чинників, серед яких не останнім є стан системи інформаційної безпеки. Дехто з науковців вважає, що має місце «фактична відсутність в Україні системи інформаційної безпеки, яка б забезпечувала не тільки виявлення та аналіз інформаційних загроз національній безпеці, а й, що надзвичайно важливо, адекватну обстановці протидію цим загрозам».

Слід також пам'ятати, що безпечний розвиток будь-якого суспільства, держави, людини прямо пов'язаний з їхньою інформаційною безпекою, оскільки інформаційне середовище є системотворчим фактором цього розвитку.

Водночас, інформаційна безпека являє собою складну, динамічну, цілісну соціальну систему, компонентами якої є підсистеми безпеки особистості, держави і суспільства. Саме взаємозалежна, системна інформаційна єдність останніх складає якісну визначеність, покликану здійснити захист життєво важливих інтересів людини, суспільства і держави, забезпечити їх конкурентоздатний, прогресивний розвиток.

При цьому, системний підхід при аналізі феномену інформаційної безпеки означає, що всі суспільні зв'язки і опосередковування, елементи і складові суспільства й держави, функції і проблеми, котрі стосуються забезпечення інформаційної безпеки, розглядаються як взаємопов'язане ціле, а застосування системного підходу дозволить встановити загальну орієнтацію досліджень проблем інформаційної безпеки й зафіксувати науковими засобами цілісність, організованість об'єкта (системи, проблеми, соціального явища, процесу тощо), що досліджується, в усій його повноті та в усій багатоманітності й поліаспектності зв'язків в об'єкті.

Слід звернути увагу, що більшість суб'єктів системи інформаційної безпеки також є її об'єктами – людина і громадянин, держава, окремі її органи, інститути тощо. Власне тому, вважаємо за потрібне говорити про об'єктно-суб'єктний склад як елемент системи інформаційної безпеки. Аналіз наукових досліджень і законодавчих норм свідчить про плюралізм підходів до суб'єктного складу системи забезпечення інформаційної безпеки.

Забезпечення інформаційної безпеки можна визначити як комплекс адміністративних заходів необхідний для досягнення такого стану інформаційного розвитку (духовного, соціально-політичного, технічного) та захищеності особи, суспільства, держави, за якого сторонні інформаційні впливи не завдають суттєвої шкоди національним інтересам. Діяльність із забезпечення інформаційної безпеки має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства та людини за трьома головними напрямами:

– інформаційно-психологічному, зокрема щодо забезпечення конституційних прав і свобод людини й громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі для утвердження загальнолюдських та національних моральних цінностей;

– технологічного розвитку, зокрема стосовно розбудови та інноваційного оновлення національних інформаційних ресурсів, упровадження новітніх технологій створення, оброблення та поширення інформації;

– захисту інформації, зокрема щодо забезпечення її конфіденційності, цілісності й доступності, в тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак.

Література

1. Інформаційна безпека людини:теорія і практика: моногр. / Золотар О. О. – Київ : ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.

2. Система забезпечення інформаційної безпеки України // Національна безпека і оборона. – 2001. – №1. – С. 16-28.

УДК 347.77

Пуркар Д.П.
Березньова А.О.
Трофименко Н.С.
Настрадін В.П.
кандидат технічних наук, професор,
Національна академія Служби безпеки України

ПРОБЛЕМИ ПРАВОВОГО РЕЖИМУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

Сьогодні, під час переходу до ринкових відносин, відбувається посилення конкуренції між суб'єктами господарювання, а рівень конкурентоздатності залежить також і від уміння окремого суб'єкта господарювання захистити свою комерційну таємницю від її неправомірного використан-

ня. Тому виникає нагальна необхідність правового захисту комерційної таємниці, через те, що її розголошення може завдати збитків, адже в Україні дотепер відсутній повноцінний правовий механізм захисту такої інформації.

Організація та технологія конфіденційного діловодства, на жаль, сьогодні ще не регламентовані державними нормативними актами. Їх визначає власник конфіденційної таємниці, беручи до уваги специфіку роботи приватного підприємства. В той же час існує необхідність керуватися визначеними нормами та правилами роботи з конфіденційними документами, адже вони забезпечують належний рівень функціонування підприємства, конфіденційність інформації та збереженість таких документів.

Саме недоліки чинного законодавства створюють труднощі та проблеми для володільців комерційної таємниці, а також обмежують можливості реалізації та захисту їх права на таку інформацію. Через це відбувається поширення комерційного шпигунства та безперешкодне використання незаконно отриманої комерційної таємниці.

У нашій державі керівництво підприємства на власний розсуд може створити окрему службу (відділ) безпеки підприємства, в обов'язки якої входить контроль поширення інформації, що становить комерційну таємницю.

Щодо законодавчого забезпечення захисту комерційної таємниці в Україні, то існує багато аспектів, серед яких найважливішими є визначення правового положення комерційної таємниці як соціального ресурсу, юридичне закріплення права на комерційну таємницю та створення правових гарантій реалізації цього права, регулювання відносин, які виникають у сфері обігу комерційної таємниці.

Необхідність прийняття закону України про комерційну таємницю обумовлена такими чинниками:

1) розвитком підприємництва в Україні та посиленням економічної конкуренції на товарних ринках;

2) практичною потребою в узаконенні суспільних відносин, які виникають у зв'язку з комерційною таємницею, а також які не врегульовані нормами права;

3) відсутністю законів, здатних виконати функцію узаконення суспільних відносин у сфері комерційної таємниці;

4) приведенням українського законодавства відповідно до світового у сфері захисту комерційної таємниці.

Згідно із статтею 6 Закону України «Про доступ до публічної інформації» і статтею 21 Закону України «Про інформацію» комерційна таємниця є інформацією з обмеженим доступом [1, 2].

Будь-яка інша інформація вважається відкритою. Обмеження доступу до комерційної таємниці відбувається відповідно до закону при дотриманні визначених вимог, а саме це може бути виключно в інтересах націона-

льної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Також розголошення інформації може завдати істотної шкоди цим інтересам та шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Дослідження особливостей роботи з документами, які містять комерційну таємницю, дозволяє обґрунтувати ряд основних вимог обліку конфіденційних документів.

Заходи захисту комерційної таємниці можна розділити на 3 групи: нормативно-правові, організаційні та технічні. Отже, охороняти комерційну таємницю повинні не лише її володілець (керівник установи, в якій цю інформацію було визначено комерційною таємницею), а й органи державної влади. Також не останню роль в охороні комерційної таємниці відіграє служба діловодства на підприємстві, яка відповідає за ведення єдиного порядку обліку, руху та зберігання документів. За правопорушення у сфері обігу комерційної таємниці законодавством визначено дисциплінарну, адміністративну, цивільно-правову та кримінальну відповідальність.

Найбільш важливими є дослідження проблем нормативно-правового забезпечення охорони документів, які містять комерційну таємницю. Загалом окремого Закону України, де було б визначено всі поняття, систематизовано процедуру захисту та регламент роботи з комерційною таємницею не існує, хоча статтею 21 Закону України «Про інформацію» визначено, що «відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом» [3].

Цивільний кодекс України, визначаючи перелік майнових прав, пов'язаних з правом інтелектуальної власності щодо комерційної таємниці (ст. 506), не встановлює правового режиму комерційної таємниці, порядку віднесення інформації до комерційної таємниці, підстав виникнення прав суб'єктів на комерційну таємницю, порядку доступу до комерційної таємниці тощо. Таким чином, вдосконалення правового регулювання відносин щодо визначення, поширення, збереження та захисту комерційної таємниці – прерогатива спеціального закону, який на сьогодні відсутній.

Отже, чинне законодавство не встановлює заходів захисту комерційної таємниці, не визначає конкретний механізм реалізації прав власників комерційної таємниці. Недосконалість законодавства позбавляє власників інформації, яка відноситься до комерційної таємниці, належного захисту своєї власності, обмежує можливість реалізації прав особи щодо інформації з обмеженим доступом, яка створюється в процесі діяльності суб'єктів, завдає матеріальної та нематеріальної шкоди власникам комерційної таємниці, що також пропонується врахувати у проекті нового закону.

Література

1. Закон України Про інформацію // ВВР від 01.12.1992. – № 48. – Ст. 650.
2. Закон України Про доступ до публічної інформації // ВВР від 12.08.2011. – № 32. –1491 с. – Ст. 314.
3. Цивільний кодекс України // ВВР, 2003. – № 40-44. – Ст. 356.

УДК 336.744

Романова Т.В.
Хоменко О.А.
Національна академія Служби безпеки України

ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ ЗАСТОСУВАННЯ КРИПТОВАЛЮТ В УКРАЇНІ

Глобальні фінансові кризи, розвиток фінансових технологій і здешевлення вартості послуг і візуалізації інформації сприяли виникненню власної валюти та роздрібних платіжних систем. Світова економічна криза висвітлила кілька ключових проблем, зокрема активний вплив політики на економіку та неефективність використовуваних фінансових механізмів. У результаті такий вплив став поштовхом для створення нових технологій, покликаних підвищити ефективність функціонування фінансової сфери. Одним із таких можливих інструментів є блокчейн-технології. Поява біткойна стала знаковою інновацією і, яку нині прийнято вважати однією із актуальних тем сучасного цифрового світу.

Використання Blockchain як технологічної інновації сприятиме побудові ефективних і прозорих систем для відстеження та реєстрації фінансових операцій та підвищенню ефективності функціонування фінансової сфери, оскільки блокчейн дозволив би працювати без посередництва третьої сторони з достатнім рівнем безпеки. Отже, враховуючи переваги технології «блокчейн», широке її впровадження неминуче, однак для цього потрібен певний час. Wedbuch прогнозує, що до 2025 р. лише 10 % карткових онлайн-платежів і 20 % міжнародних грошових переказів приватних осіб будуть виконуватися з використанням блокчейн-технологій.

Із блокчейн-технологіями пов’язують виникнення безлічі різних стартапів і компаній, що працюють на базі блокчейн-технології або побічно пов’язаних з нею, наприклад, такі стартапи, як Coinbase – криптовалютна біржа, де можна купувати і продавати біткойни, а також користуватися послугами зі зберігання і захисту цифрових активів.

Водночас, попри очевидні переваги технології «блокчейн» перейти на нову технологію вдасться не так швидко. Передусім – невизначеність у правовій та регуляторній сферах. Крім того, широкомасштабне впровадження цієї технології потребуватиме значних зусиль у частині стандарти-

зації та уніфікації. Потрібно також побудувати багаторівневу інфраструктуру «блокчейн» і зміцнити довіру до неї споживачів і регуляторів [1, с. 68-78].

На сьогоднішній день у Верховній Раді зареєстровано законопроект №7183 [2], яким вносяться зміни до Закону «Про Національний банк України». Передбачається, що державне управління у сфері обігу криптовалют буде покладено на Національний банк України.

Автори законопроекту вказують на те, що Україна входить до країн-лідерів у сфері застосування криптовалюти і технології блокчейн та є ідеальним місцем для розвитку новітніх технологій [2]. До криптовалюти застосовуватимуться загальні норми які поширюються на право приватної власності. Згідно із законопроектом держава не відшкодовуватиме вартість криптовалюти у разі її знецінення або втрати з будь-яких інших причин.

В Україні насамперед має бути впроваджено ліцензування підприємницької діяльності з віртуальною валютою. При цьому ліцензії мають надаватися лише за умови забезпечення захисту прав споживачів, запобігання відмиванню грошей і підвищення вимог до кібербезпеки при роботі з криптовалютами. З метою детінізації даного сектору необхідно внести зміни до Податкового кодексу України щодо включення доходів від здійснення операцій з віртуальною валютою до об’єктів оподаткування податком на доходи фізичних осіб. Крім того, організації, які працюють з віртуальними валютами в Україні, мають звітувати про підозрілі операції своїх клієнтів, що сприятиме дотриманню Міжнародних стандартів з протидії відмиванню коштів та фінансуванню тероризму і розповсюдженню зброї масового знищення FATF. Отже, це забезпечить реалізацію завдань Комплексної програми розвитку фінансового сектору України до 2020 року, пов’язаних з необхідністю впровадження фінансових і технологічних інновацій та забезпечення прозорості [3, с.10].

Найбільш гострою постає проблема застосування кримінальної відповідальності за дії, вчинені із застосуванням криптовалют. Прикладом цього є рішення Окружного суду Флориди, у якому суд дійшов висновку про те, що будь-який незначний продаж біткойна тому, хто планує використовувати його в злочинних цілях, не є достатньою основою для обвинувачення в легалізації (відмиванні) доходів, отриманих незаконним шляхом, навіть при тому, що злочинний намір є очевидним при продажі криптовалюти.

В результаті нашого дослідження аналіз показав, що у будь-якому разі криптовалюта – це перспективна технологія, і вона буде розвиватися незважаючи на спротив чи нерозуміння.

Щоправда, український чиновник ще не готовий до таких речей через видові особливості психіки. Адже навіть на цьому етапі розвитку криптовалюти можуть скласти конкуренцію національній валюті щодо надійнос-

ті чи навіть міжнародної валютної ліквідності. Але з іншого боку, сьогодні вже працюють декілька ініціативних груп спеціалістів IT-бізнесу, юристів та економістів, які розробляють відповідні нормативні ініціативи. Маємо надію на те, що бізнес-середовище зуміє знайти і запропонувати державі компромісні підходи, за якими криптовалюти в Україні будуть не маргінальним феноменом, а цивілізованим фінансовим інструментом.

Література

1. Волосович С. В. Віртуальна валюта: глобалізаційні виклики і перспективи розвитку / С. В. Волосович // Економіка України. – 2016. – № 4. – С. 68-78.

2. Проект Закону про обіг криптовалюти в Україні № 7183 від 06.10.2017 / [Електронний ресурс]. – Режим доступу http: //w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684.

3. Про надання дозволу Державній службі спеціального зв'язку та захисту інформації проводити перевірки стану криптографічного захисту інформації: розпорядження Кабінету Міністрів України № 373-р від 15 квітня 2015 р. // Урядовий кур'єр. – 2015. – 18 червня. – С. 10.

УДК 004.056

Савченко В.А.
Інститут підготовки юридичних кадрів для СБ України
Національного юридичного університету ім. Ярослава Мудрого

АКТУАЛЬНІ ПИТАННЯ СИСТЕМИ ПІДГОТОВКИ КАДРІВ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ TOPICAL ISSUES OF THE TRAINING SYSTEM IN THE FIELD OF INFORMATION SECURITY

[5]The system of information security specialists' training and retraining, which developed in Ukraine in the second half of the 1930's, is currently undergoing a new transformation and modernization taking into account modern requirements for information security (IS) and, as a consequence, the level of specialists' training. Increasing opportunities for unauthorized access to information expansion, due to the emergence of new competitors, organizations and individuals tat are interested in unauthorized access to information; the emergence of additional channels of information leakage, first of all, in the process of processing it by means of electronic computers; the use of new methods and means of unauthorized access to information considerably complicated the conditions for its protection, especially in terms of countering technical intelligence and preventing unauthorized modification of information in automation the systems of data processing by infecting it with viruses and software bookmarks of different types authorized by the receiving of information; safety in the conditions constantly changing and complicated, requires the constant conduction of

fundamental and applied research, phenomena and processes in this subject. A certain number of well-trained and competent specialists in this sphere is also needed.

[1]The consequence of this process was the emergence of some modifications and trends in the system of information security specialists' training and advanced training. So, the following goals in this area should be satisfied:

- training and retraining of specialists who are capable to solve modern information security tasks effectively;
- an increase in the number of specialists who have to be trained and retrained;
- bringing together the efforts of leading educational, research and administrative teams to solve large-scale problems of information security personnel's training and retraining.

Consequently, it is necessary to consider the category of formation and development of the system of IS personnel's training in both the USSR and Ukraine to its current state within the framework of the first part. It is also necessary to analyze the normative documents defining the system of education, their actual execution, the formation of a network of educational institutions in the field of IS personnel's training. The study of normative documents and the actual state of affairs suggests that the system of IS personnel's training as of 2005 included the training of specialists with higher education in five specialties: 1601.01 "Protection of limited information and automation of its processing" (in computer systems), 1601.02 "Protection of information with limited access and automation of its processing", 1601.03 "Protection systems against unauthorized access", 1601.04 "Administrative management in the field of protection of information with restricted access" and 1601.05 "Information protection in computer systems and networks" in 32 higher education institutions of Ukraine, and the training of specialists with secondary specialized education was not done at all.

[3]Since 2005, in connection with the reorganization and harmonization of the Soviet system of education with European criteria and standards, the practical accession to the Bologna process, the classification of specialties has been changed: 1701.01 "Security of information and communication systems", 1701.02 "Systems of technical information protection" and 1701.03 "Information management", as well as the introduction of training levels such as: bachelor, specialist and master.

[2]Let us accentuate on the factors that determine the concept of professionals' training. The most important factors include:

- a sharp increase of volume and composition of information that needs protection, and the necessity to increase the reliability of its protection;
- the necessity to improve the quality of specialists' training in connection with the complication of conditions for the protection of state secrets, the

specifics of protection commercial secrets, the emergence of channels of information leakage through technical means of receiving and processing information etc.;

- the necessity to use all forms of education (training, advanced training, retraining) to fill the needs in having IS specialists;
- the necessity of using a differentiated approach in specialists' training, which is dictated by the fact that nowadays there is a need in both universal specialists in integrated information security and specialists in the certain areas of information protection (organizational, legal, engineering, programmatic and mathematical) and specialists who take into account sector specifics (telecommunication and communication, aviation communication, control systems, etc.), for the preparation of which new specialization and training directions should be introduced.

An important link in this issue is the improvement of the skills of the already formed personnel. In the area of specialists' professional development, the essence of the impact of changes that have taken place in Ukraine is reduced to the following. It is necessary to provide the professional development of IS specialists who are specialized in protecting of state secrets, as well as commercial ones. In modern conditions there should be not only, and not even so much industry, but an inter-sectoral system of qualification improvement. Taking into account the peculiarities of specialization, the limitation of the term of education, the work of specialists in a particular area of information protection, it is expedient to differentiate learning. The advanced training duration must be also differentiated depending on the direction of protection (from two weeks up to two months).

The program of retraining and advanced training should have a practical orientation, clearly defined aim and tasks. According to it, IS executives and employees must attend advanced training courses at least once every 3 years, and specialists, who are first admitted to public service, have to attend them during the first year of their work in professional programs. After graduation, all students receive a certificate of advanced training.

One of the main tasks of training, along with the increase of professional qualification, is the formation of an appropriate attitude to the practical activity of ensuring information security, initiative and creative attitude to the assigned business. [4]The main aim of training should consist of training IS specialists who have the necessary qualifications; development and implementation of measures to provide IS, as well as continuous monitoring of its compliance and the required amount of knowledge and skills which must be mastered.

Thus, in our view, retraining and advanced training of specialists in information security in Ukraine should be conducted within a single curriculum.

For this purpose, it is offered:

- to determine the list of universities in which such training should be carried out, since today almost all interested persons carry out the IS specialists' training;

- to determine the directions of IS specialists' advanced training and retraining;
- to determine the list of educational establishments, which should be in charge of carrying out advanced training and retraining of specialists.

To sum up, the standards define requirements for specialists in specialties, directions and sphere of activity, requirements for specialists' knowledge and skills. In addition to this, they define the disciplines in the mentioned above directions of training.

Література

1. Горбулін В. Актуальні проблеми системного забезпечення інформаційної безпеки України / В. Горбулін, М. Биченок, П. Копка // Форми та методи забезпечення інформаційної безпеки держави :збірник матеріалів науково-практичної конференції (м. Київ, 13 березня 2008 р.). – К. : Видавець Захаренко В.О., 2008. – 216 с.

2. Тихомиров О. Забезпечення інформаційної безпеки: теоретико-правовий аспект / О. Тихомиров // Право України. – 2011. – № 4. – С. 252-259.

3. Нижник Н.Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навчальний посібник [Н.Р. Нижник, Г.П. Ситник, В.Т. Білоус]; за заг. ред. П.В. Мельника, Н.Р. Нижник. – Ірпінь, 2000. – 304 с.

4. Забезпечення інформаційної безпеки цифрових програмно-керованих АТС: навчальний посібник / [Кононович В.Г., Стайкуца С.В., Тардаскіна Т.М., Шинкарчук Т.М.]; за ред. чл.-кор. В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – 168 с.

5. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності / О.Л. Морозов // Віче. – 2007. – № 12.

УДК 316.422

Сенатор Р.М.
Національна академія Служби безпеки України

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

Ми живемо в епоху інформаційного суспільства, коли інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, суспільства та держави в цілому. Оскільки критичні вразливості в програмному забезпеченні та автоматизованих системах викликають небезпідставні побоювання, то не дивно, що уряди та суспільство в усьому світі шукають кращих заходів і методів для захисту даних Інтернет-ресурсів від кіберзагроз.

На перший погляд може здатися, що кібератаки не можуть завдати великої шкоди та не забирають людських життів, але це лише на перший погляд. Розглянемо більш детально, до яких наслідків може призвести кожна з кібератак, що використовуються під час проведення кібероперацій:

вандалізм — атака, яка, звісно, не вбиває людей, але завдає удару по авторитету держави як у світі, так і серед населення, простими слова-

ми, завдає репутаційних втрат [1]. До таких кібернетичних атак можна віднести псування офіційних Інтернет-сторінок, заміну змісту образливими чи пропагандистськими малюнками;

пропаганда — розсилка спаму, що містить інформацію пропагандистського характеру, фейкові новини для просування вигідної точки зору та дезорієнтації населення [1]. А тепер уявімо, якби не було пропаганди на території Криму, в Луганській та Донецькій областях, – чи знайшла б країна-агресор таку підтримку серед місцевого населення в 2014 році? Ні! Пропаганда за допомогою масових комунікацій та кібератак почалася ще задовго до 2014 року, велася постійно й була зосереджена на певній верстві населення, так званій цільовій аудиторії;

збір інформації — злом приватних сторінок або серверів баз даних для збору цінної інформації та її заміни на інформацію, корисну іншій стороні [1]. У цьому випадку дезінформація та викрадення даних, наприклад, відомостей щодо пересування українських військ у районі ведення бойових дій, призведе до неминучих людських втрат. Інша назва – *кібершпигунство*;

відмова сервісу – атаки з великої кількості комп'ютерів, основна мета яких – порушення функціонування сайтів або комп'ютерних систем [1]. Уявімо таку ситуацію, коли в комп'ютерній системі, яка відповідає за обробку даних, отриманих з лінії розмежування, почалися збої та помилки в роботі, наслідком цього може стати те, що командир не зможе швидко прийняти правильне управлінське рішення;

атаки на об'єкти критичної інфраструктури – атаки на комп'ютери та системи, що забезпечують життєдіяльність міст, а саме: системи водопостачання, електроенергії, транспорту тощо. Цей випадок не потребує прикладів, оскільки ми самі можете уявити жахливі наслідки, бо функціонування держави і всього суспільства залежить від дієздатності таких систем [1].

Ймовірність повторних кібертак дуже висока. Це – системна проблема, а не точкова. Невірною є думка, що всі кібератаки мають один напрям: вони, як і хвороби, бувають абсолютно різними. Існує, як мінімум, із два десятки напрямів, за якими можуть здійснюватися напади і впливи на існуючу інфраструктуру. Та й причини впливів абсолютно різні: від легких, практично непомітних, до масових і деструктивних за своєю суттю, спрямованих на знищення інфраструктури.

Тож виникає питання: Як протидіяти таким серйозним реальним та потенційним загрозам? В Україні існує чітка нормативно-правова база яка регулює окреслені питання: Конституція України, закони України «Про національну безпеку», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, Доктрина інформаційної без-

пеки України. Крім того, події 2013-2014 рр. спонукали до створення Стратегії кібербезпеки України. Метою даної стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства, держави.

Проте, слід зазначити, що особиста кібербезпека є основною складовою кібернетичної безпеки держави. Будь-який співробітник, будь-якої організації, який використовує для роботи сучасні ІТ-інструменти, створюють ще одну небезпеку. Використання віддаленого доступу з особистих пристроїв та хмарного сховища стало невід'ємною частиною повсякденного життя, а втрата смартфона чи ноутбука – звичайна ситуація. Крім того, кібератаки різного характеру на персональні пристрої – не виключення. Тому виникає нагальне питання формування у суспільства інформаційної культури та дотримання основних правил особистої кібернетичної безпеки.

Отже, кіберпростір на сьогоднішній день відіграє велику роль у забезпеченні інформаційної безпеки людини, суспільства, держави. За останній час Україна зробила прогресивні кроки у створенні ефективної національної системи кібербезпеки. Але цього виявляється не достатньо для повного подолання кіберзлочинності в нашій країні. Виникає питання щодо необхідності підвищення обізнаності населення щодо кіберзагроз, збільшення кількості кваліфікованих спеціалістів у цій сфері.

Література

1. Кібербезпека як важлива складова всієї системи захисту держави. Міністерство оборони України. [Електронний ресурс] - Режим доступу : http://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html (Дата звернення : 01.03.2019 р.)

2. Законодавство України. [Електронний ресурс] - Режим доступу : https://zakon.rada.gov.ua/laws (Дата звернення : 01.03.2019 р.).

УДК 341.123

Собчак Р.А.
Національна академія Служби безпеки України

"25 КАДР" – МІФ ЧИ РЕАЛЬНИЙ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИЙ ВПЛИВ?

У 2014 р. Україна зазнала прямої агресії з боку Російської Федерації. Спочатку було анексовано АР Крим, згодом – Донецьку та Луганську області. Водночас ще задовго до загострення ситуації, що перетворилася у збройне протистояння, проти України розпочалась інформаційна війна. Форми, методи, технології та засоби її ведення, з одного боку, вважаються

простими, навіть примітивними, з другого – ця війна була давно спланована, розроблена й досить успішно реалізована.

Існує багато різновидів методу ведення інформаційно-психологічної війни та соціального впливу (дезінформування та маніпулювання; пропаганда; диверсифікація громадської думки; психологічний та психотропний тиск). Слід зазначити, що за 5 років війни науковці та фахівці доклали достатніх зусиль на виявлення та протидії таким методам інформаційного впливу, проте питання впливу на підсвідомість залишається відкритим.

В інформаційній агресії проти України були застосовані методи психотропної дії, а саме використання забороненої технології 25-го кадру. «У травні 2014 року, у Службі безпеки України заявили про те, що мають докази використання російськими телеканалами технології «25-го кадру» для інформаційно-психологічного впливу на глядачів. На той час начальник прес-служби СБУ Марина Остапенко продемонструвала журналістам відеофрагмент випуску новин на телеканалі «Росія-24», в якому використовується маніпулятивна технологія. Так, протягом усього випуску про події в Одесі 2 травня 2014 року в куті екрана з'являються малопомітні написи: «підпал: «Правий сектор», «людей убивають бандерівці», «нацгвардія – вбивці». СБУ також вдалося встановити, що російські ЗМІ використовують інші методи впливу на глядачів: поширюють напівправду, показують деталізовані сцени вбивств і насильства й намагаються емоційно впливати на глядача [1].

Отже, обробка підсвідомості людини або групи людей за допомогою навіювання чи спеціальних технічних засобів і прийомів, завдяки яким вони програмуються на беззастережне підпорядкування будь-чиїм наказам, на вчинення будь-яких дій, або на сприйняття навіювання політичної, чи релігійної доктрини, сепаратистських або терористичних переконань.

«25 кадр» - методика впливу на свідомість і підсвідомість людини за допомогою вставки прихованої реклами чи іншої інформації у вигляді додаткових кадрів. Більшістю вчених 25 кадр вважається фікцією, а сам автор методу Джеймс Вікері публічно зізнався в підробці результатів. Однак, фахівці у цій галузі стверджують: переглядаючи фільми або телепередачі, практично кожна людина піддається впливу 25-го кадру. Подібний інструмент, на думку експертів, може бути одночасно і потужною зброєю впливу, що використовуються для благих цілей, і пропагандою негативних вчинків. Вся справа в тому, що людина не може сприймати зображення, що з'явилося на екрані, але відкладає дані у свою підсвідомість. Як відомо, для того щоб людське око при проекції кінофільму або телепередачі не помічав переходу від одного кадру до іншого, за секунду повинні мінятися 24 кадри. Так званий "25-й кадр" неможливо вловити оком, але психологи давно знають, що він має дуже потужним сугестивний вплив і тому його використання заборонено.

Слід зазначити, що частота 25 кадрів в секунду стала предметом обговорень дитячих психологів, а небайдужі люди навіть створили відеоролик, в якому пояснюють вплив даного ефекту на дітей. Особливо сильно дістається тим мультфільмів, які виробляє «Дісней», наприклад «Шреку». Хоча вплив 25-го кадру на дитячу психіку до кінця не вивчена, а тому психологи рекомендують уважніше підбирати мультфільми для дітей [2].

Крім того, проблема «25 кадру» вбачається ще й у використанні прихованої реклами, а це у свою чергу відповідно до ст. 9 ЗУ «Про рекламу» використання прихованої реклами заборонено. Саме поняття в ст. 1 цього закону визначається так: «Прихована реклама – це інформація про особу чи товар у програмі, передачі, публікації, якщо така інформація слугує рекламним цілям і може вводити в оману осіб щодо дійсної мети таких програм, передач, публікацій» [3]. Фахівці наголошують на тому, що визначення поняття «прихована реклама» в українському законодавстві неточне. По-перше, воно не містить переліку характерних ознак прихованої реклами. По-друге, є дуже подібним до визначення поняття «недобросовісна реклама»

Які несе 25 кадр наслідки для людини:

кодування підсвідомості – в прихованому кадрі можна помістити будь-яку інформацію, як позитивну, так і негативну, яка провокує людини на певні дії;

мелькання зображення – у людей з нестабільною психікою може викликати афекти, психози, у епілептиків – припадки.

Отже, з огляду на вищевикладене, можна дійти до таких висновків:

За допомогою інформаційного впливу на людську підсвідомість, можна з легкістю керувати як людиною, так і групою людей. Вчені постійно працюють над різноманітними теоріями не лише для того, щоб товар купувався чи не купувався, а для того, щоб запобігти масовим заворушенням.

На жаль увесь масив телереклами та фільмів із закладеним в них 25 кадром уповноважені на те суб’єкти не в змозі переглянути та не допустити на ТВ. Тож нам залишається лишень постійно бути на сторожі і дбати про те інформаційне поле, яке нас оточує і критично сприймати тих, хто його монтує.

Література

1. У СБУ заявили, що російські канали застосовують проти телеглядачів «25-й кадр» [Електронний ресурс]. – Режим доступу : http://tsn.ua/politika/u-sbuzayavili-schorosiyski-kanali-zastosovuyut -protiteleglyadachiv-25-y-kadr-350517.html.

2. 25 кадр - це що таке? Суть, ефект, вплив 25-го кадру на людину [Електронний ресурс]. – Режим доступу : http://hi-news.pp.ua/tehnka-tehnologyi/11720-25-kadr-ce-scho-take-sut-efekt-vpliv-25-go-kadru-na-lyudinu.html.

3. ЗУ «Про рекламу» N 2484-VIII (2484-19) від 03.07.2018.

УДК 351.746.1(477): 001.8
Терещук В.В.
Національна академія Служби безпеки України

МЕТОДОЛОГІЧНИЙ ПІДХІД ДО ФОРМУВАННЯ СИСТЕМИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Оборона України, захист її суверенітету, територіальної цілісності і недоторканності покладаються на Збройні Сили України, а забезпечення державної безпеки і захист державного кордону України – на відповідні військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом [1].

Відповідно до Указу Президента України від 26.05.2015 № 287/2015 «Про рішення Ради національної безпеки і оборони України від 06.05.2015 «Про Стратегію національної безпеки України» серед основних загроз національній безпеці України є агресивні дії Російської Федерації, що здійснюються на виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території [2]. Як відомо, у зв'язку із черговим актом збройної агресії з боку Росії проти кораблів Військово-Морських Сил України в азовсько-чорноморському регіоні, а також наявною загрозою широкомасштабного вторгнення в Україну збройних сил Росії, Указом Президента України № 393/2018 з 26.11.2018 (на 30 діб) в нашій державі було введено воєнний стан. Враховуючи викладене, дослідження з цієї проблематики є актуальним та своєчасним.

Так, основним нормативно-правовим актом, що визначає напрями діяльності держави у сфері забезпечення національної безпеки є Закон України «Про національну безпеку України», який визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз. Конкретні засоби і шляхи забезпечення національної безпеки України обумовлюються пріоритетністю національних інтересів, необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз цим інтересам і ґрунтуються на засадах правової демократичної держави.

Варто зазначити, що загрози національній безпеці України це – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [3].

На сьогодні національна безпека України є однією з найголовніших сфер відповідальності держави і вимагає до себе уваги з боку не тільки

спеціальних державних органів, а й «непрофільних» міністерств і відомств, помилки в діяльності яких можуть становити загрозу ефективній реалізації національних інтересів України. Діяльність у сфері національної безпеки має бути скоординованою і здійснюватися у єдиній «системі координат». Засади для цього треба закласти у методологічному підході до аналізу національних інтересів і загроз їхній реалізації, визначення функцій і структури системи забезпечення національної безпеки. Ці засади мають відповідним чином закріплюватися в законодавстві України і становити норми діяльності органів державної влади.

Складовими методологічного підходу мають бути методи визначення національних інтересів, аналізу загроз, формування функцій та визначення пріоритетів діяльності системи забезпечення національної безпеки України. В методологічному підході національні інтереси розглядаються як базовий об'єкт забезпечення національної безпеки. Вони є орієнтирами суспільного розвитку, значною мірою мають впливати на визначення його напрямів і пріоритетів [4, с. 92-94].

Отже, на нашу думку національні інтереси України – це суспільно визнанні (за допомогою референдумів, виборів тощо) і законодавчо оформлені потреби людини, суспільства, держави, реалізація яких забезпечує всім названим соціальним суб'єктам стабільне співіснування, ефективне функціонування, прогресивний розвиток у рамках багатонаціональної держави.

Під потребою держави в захисті національних інтересів розуміється необхідність у такому діапазоні станів держави, суспільства, його структур, а також оточення, коли досягається гарантоване забезпечення умов реалізації національних інтересів за наявності умов або передбачення загроз [5, с. 117-119].

У аспекті питання, яке розглядається важливо зазначити, що визначення методологічних засад у сфері забезпечення національної безпеки дає можливість на новому якісному рівні: а) перейти до оптимізації системи забезпечення національної безпеки, організації ефективної системи моніторингу зовнішньої та внутрішньої обстановки; б) прогнозувати зміни умов і чинників, що впливають на стан національної безпеки; в) визначити шляхи та заходи щодо запобігання і локалізації загроз національним інтересам; г) обґрунтувати пріоритети політики національної безпеки України.

Враховуючи викладене, система забезпечення національної безпеки України – це організована державою сукупність суб'єктів (державних органів, громадських організацій, посадових осіб, громадян та їх спілок), які об'єднані цілями та завданнями щодо захисту національних інтересів і здійснюють свою діяльність у цій сфері відповідно до визначених у законодавстві України функцій, механізмів їх виконання.

Потенційними джерелами отримання ефекту від використання запропонованого методологічного підходу можуть бути:

- можливість випереджувальної та адекватної реакції стосовно загроз національним інтересам України за рахунок використання прогнозних оцінок у сфері національної безпеки;

- запобігання можливим негативним наслідкам від прояву загроз та прийняття недосконалих рішень у сфері національної безпеки.

Завдяки використанню системних принципів під час розробляння методології, вона має досить загальний характер. Це дає можливість використання запропонованого підходу не тільки стосовно системи забезпечення національної безпеки, а й під час вирішення проблем реформування управлінських і виконавчих структур в інших сферах життєдіяльності суспільства, держави.

Таким чином, застосування методологічних підходів до формування системи національної безпеки України надасть можливість законодавцю оптимізувати систему забезпечення національної безпеки нашої держави та чітко обґрунтовувати пріоритети її політики.

Також подальші дослідження будуть спрямовані на аналіз загроз національної безпеки України.

Література

1. Конституція України // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

2. Указ Президента України від 26.05.2015 № 287/2015 «Про рішення Ради національної безпеки і оборони України від 06.05.2015 «Про Стратегію національної безпеки України» Режим доступу: https://zakon.rada.gov.ua/laws/show/287/2015.

3. Закон України «Про національну безпеку України» // Відомості Верховної Ради України, 2018. - № 31. – Ст. 241.

4. Теоретико-методологічні засади забезпечення національної безпеки держави у її визначальних сферах : монографія / В.Ю. Богданович, А.І. Семенченко, Ю.В. Єгоров, О.О. Бортник, В.А. Муха. – К. : Кий, 2007. – 370 с.

5. Баланда А.Л. Соціальні детермінанти національної безпеки України: Монографія. – Інститут демографії та соціальних досліджень НАН України. К., 2008. – 414 с.

УДК 004.056.5:342.7:347.965

Троян А.П.
Науково-дослідний інститут інформатики і права
НАПрН України

АКТУАЛЬНІ ПРОБЛЕМИ РЕАЛІЗАЦІЇ ПРАВА НА ПРОФЕСІЙНУ ПРАВНИЧУ ДОПОМОГУ В УМОВАХ ЗАБЕЗПЕЧЕННЯ РЕЖИМУ СЕКРЕТНОСТІ

Гарантіями статті 59 Конституції України встановлено, що кожен має право на професійну правничу допомогу. Кожен є вільним у виборі захисника своїх прав.

Питання реалізації права на професійну правничу допомогу в умовах забезпечення режиму секретності традиційно досліджувалися в розрізі кримінального процесу, адже до 01 січня 2019 року (до набрання чинності

окремих положень Закону України «Про внесення змін до Конституції України (щодо правосуддя)») представництво учасників судового процесу (цивільного, господарського, адміністративного) в судах першої інстанції здійснювалося не лише адвокатами, а й іншими особами відповідно до вимог процесуального закону.

Оскільки представником в інших судових процесах міг бути фахівець в певних галузях права або взагалі особа, яка не має професійної правничої освіти, - можливість участі у справі представника, який має допуск до державної таємниці, без звуження його фаху, була більш широкою.

Таким чином, на сьогоднішній день значно збільшилася кількість справ у цивільному, господарському, адміністративному процесах та справах про адміністративні правопорушення, в яких представником учасника процесу може бути виключно адвокат. А отже – право вільного вибору захисника своїх прав для громадянина хоча і залишилося регламентованим, але на практиці виявляється дуже проблематичним: обрати захисника, який має допуск до державної таємниці, доволі складно. Крім того – сам процес отримання допуску до державної таємниці достатньо тривалий, що може призвести до пропуску процесуальних строків і порушення права на захист.

Питання охорони державної таємниці під час кримінального провадження регулюються ст. 517 КПК України. В той же час, нормами чинних на цей час редакцій Цивільного процесуального Кодексу, Господарського процесуального Кодексу, Кодексу адміністративного судочинства та Кодексу України про адміністративні правопорушення питання охорони державної таємниці фактично не врегульовані – існують лише поодинокі приписи щодо необхідності проведення закритих судових засідань для запобігання розголошенню таємної інформації (ч. 8 ст. 10 КАС України, ч. 7 ст. 7 ЦПК України, ч. 8 ст. 8 ГПК України, ст. 249 КУпАП).

Відсутність чітких приписів законодавства щодо питань забезпечення прав учасників судових процесів у випадку розгляду справ, пов’язаних із необхідністю доступу до державної таємниці, є не лише серйозною прогалиною у відповідних процесуальних законах, а й прямо порушує права громадян як на доступ до суду, так і на вільний вибір захисника.

Так, Постановою Пленуму Вищого адміністративного суду України від 13.03.2017 року № 4 «Про Довідку щодо допуску і доступу представника позивача до матеріалів адміністративної справи, які містять державну таємницю» суддям адміністративних судів було рекомендовано застосовувати за аналогією положення кримінального процесу в частині забезпечення прав захисників (адвокатів) щодо доступу до інформації, що містить державну таємницю, до представників позивача в адміністративному процесі.

Крім того, в ході проведення судової реформи 2016-2017 років виникла ще одна проблема, яка ускладнила реалізацію права громадянина на доступ до суду, встановленого ст. 55 Конституції України.

24 жовтня 2018 року колегією суддів новоутвореного Верховного Суду у справі №9901/774/18 було зупинено розгляд справи до вирішення питання допуску до державної таємниці суддів зі складу колегії. Згідно мотивувальної частини вказаної ухвали «Відповідно до листа Департаменту охорони державної таємниці та ліцензування СБУ від 23 лютого 2018 року № 26/1/1-3259 на сьогодні у Верховному Суді немає режимно-секретного органу, а суддям Касаційного адміністративного суду у складі Верховного Суду не надано спеціальних дозволів на провадження діяльності пов'язаної з державною таємницею.».

Наявність в судах режимно-секретного органу є обов'язковою умовою надання можливості підозрюваному (обвинувачуваному) або його адвокату робити виписки з матеріалів, які містять державну таємницю. В подальшому такі виписки підлягають зберіганню саме в режимно-секретному органі суду. Такими є вимоги ст. 517 КПК України, але для інших процесів (окрім кримінального) аналогічних вимог не встановлено.

Таким чином, складається ситуація, коли міри державного примусу щодо забезпечення охорони державної таємниці спрямовані супротив гарантованих Конституцією України прав кожного на вільний вибір захисника.

На нашу думку, окреслені проблеми потребують термінового вирішення шляхом включення до процесуального законодавства положень, які б забезпечували одночасно як можливість здійснення безперешкодного, вчасного та повного доступу представників (адвокатів) до інформації, що містить державну таємницю, так і забезпечення режиму секретності.

Література

1. Про Довідку щодо допуску і доступу представника позивача до матеріалів адміністративної справи, які містять державну таємницю. – Постанова Пленуму Вищого адміністративного суду України. – [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/en/v0004760-17 – Назва з екрана.

2. Ухвала Верховного Суду в справі №9901/774/18 від 24 жовтня 2018 року. – Єдиний державний реєстр судових рішень. – [Електронний ресурс]. Режим доступу: http://reyestr.court.gov.ua/Review/77375305.

УДК: 32.019.51:323.28:323.2(477)

Трухан В.О.
Національна академія Служби безпеки України

КІБЕРТЕРОРИЗМ ЯК СКЛАДОВА ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ

Тимчасова окупація частини території та потужна інформаційна війна проти України продемонстрували нашу неготовність протистояти терори-

стичній загрозі повною мірою. Враховуючи виклики, які стоять перед Україною з початком збройної агресії, особливо в контексті інформаційної війни, існує чітке розуміння необхідності удосокналення практики і правового регулювання стану інформаційної безпеки.

Інформаційна зброя стає ідеальним засобом для терористів, а інформаційний тероризм може стати загрозою існуванню цілих держав, що робить питання інформаційної безпеки важливим аспектом національної та міжнародної безпеки.

Проблеми інформаційної безпеки стають все більш актуальними, особливо в контексті проведення антитерористичних заходів, де більшість суб'єктів боротьби з тероризмом в той чи інший момент страждають від порушень цілісності даних. Інтервали між витоками даних і виявленнями данних інцидентів збільшується, і звичайні методи запобігання втраті даних стають менш ефективними.

Семантика нормативно-правових актів дає підстави стверджувати, що поняття інформаційного тероризму не знайшло свого відображення в чинному законодавстві України, однак на доктринальному рівні означене поняття досліджувалось як юристами, так і фахівцями з державного управління, безпекознавства та політології [2].

Так, В.О.Коршунов вказує, що інформаційний тероризм – це новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави [3, с. 6].

Т.П. Яцик вважає, що сучасний інформаційний тероризм характеризується як множина інформаційних війн та спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав. Доступність інформаційних технологій значно підвищує ризики інформаційного тероризму [4, с. 57].

Міжнародні фахівці у сфері боротьби та протидії інформаційним загрозам, зазначають, що інформаційний тероризм – злиття фізичного насильства зі злочинним використанням інформаційних систем, а також умисне зловживання цифровими інформаційними системами, мережами або їх компонентами з метою сприяння здійсненню терористичних операцій або акцій [5, с. 98].

Оскільки, кібезрбезпека держави є частиною інформаційної безпеки держави, розглянемо кібертероризм як складову інформаційного тероризму.

Відповідно до ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» кібертероризм - терористична діяльність, що здійснюється у кіберпросторі або з його використанням [1].

З огляду на поточну ситуацію в країні, для системи антитерористичних заходів важливим питанням є кібертероризм, а саме – тероризм спланований, вчинений чи скоординований в кіберпросторі, тобто в терористичних акціях використовуються новітні досягнення науки і техніки в галузі новітніх інформаційних технологій. Кібертероризм є транснаціональним діянням, яке вчиняється окремими індивідами чи організаціями осіб [6].

Поки кібертероризм з розряду «потенційної» загрози не перейшов до розряду «реальної» загрози, слід застосовувати превентивні заходи для недопущення його становлення. Основою забезпечення боротьби з кібертероризмом є створення ефективної системи заходів із запобігання, виявлення та припинення такого виду злочинності. Враховуючи, що в Україні на даний момент існує низка нормативно-правових актів, що регулюють питання інформаційної безпеки в цілому, слід зазначити, що головною зброєю у боротьбі з цією загрозою залишається законодавство, яке потребує подальшого вдосконалення. Тому найбільш дієвим напрямом у вирішенні комплексної проблеми протидії кіберзлочинності у наш час є міжнародне співробітництво правоохоронних органів та спеціальних служб у сфері інформаційної безпеки на основі узгодження національного та міжнародного законодавства [6].

Література

1. Закон України «Про основні засади забезпечення кібербезпеки України»: Закон України від 05.10.2017 № 2163-VIII (в поточній редакції від 08.07.2018): [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/2163-19.

2. Банк Р.О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект/Р.О. Банк // Інформація і право. – 2016. - № 1. – С. 110-116.

3. Коршунов В. О. Політичний тероризм: інформаційні методи боротьби : автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 23.00.02 «Політична інститути та процеси» / В.О. Коршунов. – Дніпропетровськ, 2008. – 18 с.

4. Яцик Т.П. Особливості інформаційного тероризму як одного із способів інформаційноївійни // Науковий вісник Національного університету ДПС України (економіка, право). – 2014. – № 2 (65) – С. 55-60.

5. Jerrold M. From Car Bombsto Logic Bombs : The Growing Threat from Information Terrorism / M. Jerrold // NATO Libraryat : Terrorism and political violence, vol. 12, no. 2, Summer 2000. – P. 97-122.

6. Діордіці І.В. Кібертероризм як елемент дестабілізації системи стратегічних комунікацій, 2016.

УДК 004.4'801
Фараон С.І.
Національний університет оборони України
імені Івана Черняховського

ДЕФІНІЦІЙНІ ПРОБЛЕМИ ТЕРМІНОЛОГІЇ У СФЕРІ КІБЕРБЕЗПЕКИ І КІБЕРОБОРОНИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Аналіз існуючих Законів України та інших нормативно-правових актів України, ЄС, НАТО, провідних країн світу, зокрема США, свідчить про дефініційну, термінологічну та нормативно-правову невизначеність або/та розбіжність об'єктно-предметної області декількох десятків понять, що складають базовий термінологічний набір терміносистеми сфери кібербезпеки та кібероборони, зокрема таких як: "кібербезпека", "кіберзахист", "кіберзброя", "кібероборона", "кіберпростір", "кібертероризм" тощо.

Семантичне навантаження дефініції визначається описом об'єкту, предмету, їх ознак та взаємозв'язків між ними. Гармонізація термінології сфери кібербезпеки та кібероборони вимагає однакового тлумачення суті об'єкту та предмету.

Можна стверджувати, що аналіз проблем нормативно-правового, науково-технічного, організаційного і кадрового забезпечення розвитку кіберсил є актуальним для створення в Україні національної системи кібербезпеки та кібероборони із врахуванням світового досвіду.

Ряд системних та управлінських проблем слід розглянути окремо, як такі, що не забезпечують належний рівень (індекс) кібербезпеки:

відсутність системності ведення кібердій, теорії застосування сил та засобів кібероборони, взаємодії різних відомств у сфері забезпечення кібероборони держави;

відсутність в секторі оборони єдиного координуючого органу з питань забезпечення кібербезпеки та системи підготовки військового й цивільного персоналу;

проблеми кадрового забезпечення відповідних структурних підрозділів та відтік за кордон кваліфікованих спеціалістів;

зниження рівня наукового потенціалу, відсутність наукових шкіл, складнощі із методичним, науковим і технічним забезпеченням відтік за кордон кваліфікованих наукових кадрів.

Вирішення вище перерахованих проблем неможливе без гармонізації та унормування термінологічних систем сфер кібербезпеки та кібероборони. На фоні не вирішення таких проблем, потенційні кіберзагрози можуть реалізуватися в успішні кібератаки на складні соціотехнічні системи держави, які призведуть до виникнення критичних ситуацій (у тому числі техногенних аварій та катастроф в енергетиці зокрема на атомних електростанціях, підприємствах хімічної, нафто - і газопереробних й інших га-

лузей, транспорті, банківській сфері та інше), наслідки від яких важко передбачити.

Терміни *кібератака. кіберзахист, кіберрозвідка, кібертероризм, кібершпигунство* – розглядаються, як це визначено в Законі [1]. Ряд дефініцій, які відсутні або некоректні в нормативно-правовому полі України можуть, на погляд автора, бути визначними так:

Кібероборона. Дефініція виразу кібероборона вимагає розуміння, що ключовим словом є оборона, а кібер - це зазначення простору, де відбуваються дії сил протиборчих сторін. Законодавчо визначена дефініція потребує корегування. Цілком зрозуміло, що політичні, економічні, соціальні, правові, організаційні заходи, які спрямовані на досягнення мети кібероборони, здійснюються не в кіберпросторі. Доцільно запропонувати наступне визначення: Кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в Державі та кіберпросторі й спрямовані на забезпечення захисту її суверенітету та обороноздатності, запобігання виникненню збройного конфлікту та відсіч збройній агресії. З урахуванням широкого застосування сучасних інформаційних технологій у секторі безпеки і оборони, створення єдиної автоматизованої системи управління Збройних Сил України оборона нашої держави стає більш уразливою до кіберзагроз [2].

Згідно Законів [3,4] оборона України, захист її суверенітету, територіальної цілісності і недоторканності, охорона повітряного простору та підводного простору держави покладаються на Збройні Сили України. Жодним Законом України кіберпростір не визначений, як середовище ведення оборонних дій для забезпечення захисту суверенітету держави. Натомість Закон України [1] встановлює, що національна система кібербезпеки включає в тому числі й оборонні заходи, а також визначає МО України та ГШ ЗСУ України завдання щодо підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); військової співпраці з НАТО та іншими суб’єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз, забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану. Розвідувальним органам України визначені завдання із здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки. А ні Законами України, а ні іншими нормативно-правовими актами не визначено перелік вичерпних заходів щодо підготовки до відбиття та відбиття воєнної агресії у кіберпросторі. Натомість, керівними документами ЗС України кібероперації розглядаються як вид самостійних операцій. Тому, для досягнення мети та безпосереднього виконання заходів у сфері забезпечення кібербезпеки сектору безпеки і оборони, визначених в [1, 5,

6, 7, 8, 9] необхідно стандартизувати та гармонізувати в нормативно-правовому полі України дефініції термінологічних систем сфери кібербезпеки та кібероборони.

Логічна операція формування значення для терміну, дефініція (лат. definitio - визначення), є важливим засобом скорочення складних описів та окремих міркувань у наукових теоріях та галузях знань, чим виконує важливу функцію у науково-освітній та практичній діяльності [10].

В термінології, як розділі лексикології, аксіомою є, що визначення будь якого терміну (дефінієндума) та зміст і значення визначаючого поняття (дефінієнса) мають бути тотожними, вичерпувати один одного і мати один і той же зміст (денотат). До науково-технічних термінів висуваються додаткові вимоги: системність, вмотивованість, однозначність, точність, відсутність синонімів [11].

З певних історичних, воєнно-наукових, зовнішньополітичних та інших причин в термінологічній системі галузі кібербезпеки та кібероборони України, склалося протиріччя, що вимагають відповідного наукового розв'язання. Воно полягає в недотриманні в термінографії сфери кібербезпеки принципів однозначності, точності та відсутності синонімів. А саме, у терміносистемі сфери кібербезпеки одночасно існує й паралельно застосовується низка дефініцій, в яких одному дефінієндуму (Dfd) ставиться у відповідність декілька дефінієнсів (Dfn), або навпаки, один дефінієнс розкриває значення різних дефінієндумів. Це ускладнюється елементами надлишковості, або недостатності денотату та відбувається на фоні жорсткої нормативно-правової легітимізації термінів, що запропоновані та втілені в обіг на рівні емоційних та емпіричних логічних операцій окремих авторів, без необхідного наукового супроводження. Термінологічна сфера кібероборони в Україні ще не сформована, тим не менш, процесу її формування притаманні ті ж самі помилки. Ускладнення цього протиріччя в площині практичного застосування термінологічного апарату сфери кібербезпеки та кібероборони відбувається за рахунок невідповідності термінологічних систем сфер кібербезпеки міжнародного співтовариства, зокрема ЄС та НАТО й України.

Вирішення протиріччя полягає у формуванні за правилами науково-технічної лексикографії множини семантичних аналітичних та синтетичних визначень термінологічної системи сфери кібербезпеки та кібероборони.

Напрямком подальших досліджень може бути формування остаточного переліку функцій та завдань суб'єктів кібероборони, систем управління, їх взаємозв'язків, критеріїв (індикаторів) загроз у сфері кібероборони держави.

Література

1. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року.

2. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015.

3. Конституція України Режим доступу: http://zakon0.rada.gov.ua/laws/show/254.

4. Закон України Про Збройні Сили України від 6 грудня 1991 року N 1934-XII (зі змінами), Режим доступу: http://zakon3.rada.gov.ua/laws/show/1934-12.

5. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015, // Урядовий кур'єр. – 2015. – № 95. [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/287/2015.

6. Концепція розвитку сектору безпеки і оборони України, введеною в дію Указом Президента України від 14.03.2016 №92/2016.

7. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96 // Офіц. вісн. України. – 2016. – № 23.

8. DOD Dictionary of Military and Associated Terms. As of January 2019. Режим доступу: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

9. Закон Про оборону України: за станом на 01.07.2018 р., затверджений ВР України від 06.12.1991, № 1932-XII . – Офіц. вид. – К.: Відомості Верховної Ради України від 03.03.1992. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1932-12.

10. Новейший философский словарь, [Електронний ресурс] — Режим доступу: https://www.google.com/search?q=chrome..69i57.9536j0j8&sourceid=chrome&ie=UTF-8.

11. Л.А. Васенко, В.В.Дубічинський, О.М. Кримець, Фахова українська мова:. Навчальний посібник. К.: Центр учбової літератури, 2008. – 272 с. [Електронний ресурс]. – Режим доступу: http://uchebniks.com/book/277-faxova-ukrayinska-mova-navchalnij-posibnik-vasenko-la/23-vimogi-do-terminiv.html.

УДК 342.6

Федоров В.Д.
Інститут підготовки юридичних кадрів для СБ України
Національного юридичного університету ім. Я. Мудрого

СУБ'ЄКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: МІЖНАРОДНИЙ ДОСВІД

Сучасні темпи розвитку інформаційних технологій не перестають вражати, втілюючи в реальність найсміливіші ідеї науковців та інженерів. Водночас, розширення комунікативних можливостей окремої людини чи певної соціальної спільноти здатне трансформуватися в нові виклики національній безпеці будь-якої держави. Україна в цьому не є виключенням, особливо з огляду на триваюче гібридне протистояння в кіберпросторі, що з боку країни-агресора характеризується постійним збільшенням масштабів кібератак та задіяних в них ресурсів, урізноманітненням форм та технологій їх здійснення з метою гарантування «гри на випередження». З огляду на це, одним з пріоритетних для України завдань є своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національній безпеці нашої держави у кіберпросторі.

Відповідно до ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» систему суб'єктів забезпечення кібербезпеки складають: 1) Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку; 2) міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [1]. Такий же перелік, але більш деталізований, міститься і в рішенні Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [2].

З огляду на це, актуалізуються питання розмежування й уточнення компетенції суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, унеможливлення дублювання їх функцій, налагодження ефективного механізму координації та взаємодії між ними, особливо в контексті державно-приватного партнерства.

Водночас, досвід провідних країн світу в цій сфері вказує на доцільність мінімізації кількості задіяних державних органів, спрощення організаційно-управлінських процедур, підвищення оперативності прийняття рішення, а в кінцевому підсумку – зменшення навантаження на державний бюджет. Наприклад, з цією метою в Німеччині діє Федеральне управління інформаційної безпеки [3;4], у Великій Британії – Національний центр кібербезпеки [5], в Ізраїлі – Національне кібербюро Ізраїлю та Національний департамент інформаційної безпеки [6], в США – координатор органів виконавчої влади з питань кібербезпеки (діє на правах помічника президента), а також Національне управління кібербезпеки при Міністерстві внутрішньої безпеки та Міністерство оборони [7].

Таким чином, ефективність протидії сучасним викликам національній безпеці нашої держави у кіберпросторі знаходиться в прямій залежності від побудови оптимальної системи задіяних в цьому суб'єктів, а також належної нормативно-правової регламентації їх повноважень.

Література

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 03.03.2019).

2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 берез. 2016 р. № 96/2016.URL: https://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 03.03.2019).

3. Gesetzüber das Bundes amt für Sicherheit in der Informations technik. URL: http://www.gesetze-iminternet.de/bsig_2009/BJNR282110009.html (дата звернення 03.03.2019).

4. Act to Strengthen the Security of Federal Information Technology. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf;jsessionid=5A1E1C722E66B37569F491E7A5D25A31.2_cid359?__blob=publicationFile (дата звернення: 03.03.2019).

5. Computer Misuse Act 1990. URL: http://www.legislation.gov.uk/ukpga/1990/18 (дата звернення: 03.03.2019).

6. Cyberwellness Profile Israel. URL: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Israel.pdf (дата звернення 03.03.2019).

7. Cyber Security Research and Development Act. URL: https://www.law.cornell.edu/topn/cyber_security_research_and_development_act (дата звернення: 03.03.2019).

УДК 351:74(437.3)

Чортополох С.Д.
Національна академія Служби безпеки України

УДОСКОНАЛЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ДОСВІД ЧЕСЬКОЇ РЕСПУБЛІКИ

В сучасному світі кожна держава усвідомлює важливість відстоювання власного інформаційного суверенітету, основою якого є інформаційні ресурси держави. Із метою урахування позитивного зарубіжного досвіду правової регламентації інформаційної сфери, розглянемо деякі особливості забезпечення інформаційної безпеки в Чеській Республіці.

За останні роки в Чехії реалізовано комплекс заходів із удосконалення забезпечення її інформаційної безпеки. Розпочато формування бази правового забезпечення інформаційної безпеки, прийнято низку законів, розпочато створення механізмів їхньої реалізації. Здійснюються певні заходи із забезпечення захисту інформації в органах державної влади, на підприємствах, в установах і організаціях усіх форм власності. Запроваджується створення захищеної інформаційно-телекомунікаційної системи спеціального призначення в інтересах органів державної влади [1].

Основним документом, що регламентує діяльність органів, які забезпечують інформаційну та державну безпеку, є «Стратегія Національної безпеки Чеської Республіки» [2]. Головним органом, що забезпечує інформаційну безпеку Чехії є Служба інформаційної безпеки (Bezpečnostní informační služba (BIS), яку було утворено 1 січня 1993 року [1].

Діяльність зазначеної служби регламентується законами Чеської Республіки «Про розвідувальні служби Чеської Республіки», «Про інформаційну безпеку» та «Про захист секретної інформації». Діяльність Служби інформаційної безпеки не є публічною, але здійснюється із суворим дотриманням законів, у тісній співпраці із поліцією, розвідкою, чеськими правоохоронними органами та правоохоронними органами країн-партнерів [2].

Відповідно до чеського законодавства Служба інформаційної безпеки здійснює аналіз процесів демократії та збереження конституційного порядку, терористичних загроз, здійснює контррозвідувальну діяльність у сфері забезпечення кібербезпеки, збирає дані щодо діяльності організованих злочинних угруповувань, забезпечує надання та законне використання стратегічно важливої розвідувальної інформації в політичній та економічній сферах. Зазначена служба є аполітичним органом, що не має репресивних повноважень, тобто не може здійснювати затримання, арешти чи допити підозрюваних. ЇЇ директор призначається на посаду Урядом Чеської Республіки після того, як його кандидатура обговорюється в комітеті Палати депутатів Парламенту Чеської Республіки, який відповідає за питання безпеки. В своїй діяльності Служба інформаційної безпеки підпорядкована та підзвітна Уряду, Прем'єр-міністру та Президенту Чеської Республіки [3].

На сьогодні основними напрямами діяльності Служби інформаційної безпеки Чехії є протидія діяльності російських та китайських спецслужб, ісламських фундаменталістів [4].

Інформаційна безпека в Чехії забезпечується шляхом розподілу повноважень між структурними підрозділами BIS та іншими спеціальними та правоохоронними органами й координації їх діяльності [1]. Значний внесок у ефективність роботи чеських спецслужб вносить міжнародне співробітництво, оскільки сучасні загрози потребують спільного та швидкого реагування.

Підсумовуючи зазначимо, що удосконалення правової регламентації забезпечення інформаційної безпеки України має відбуватися на підставі детального наукового аналізу міжнародного законодавства та відповідного досвіду інших країн, зокрема, Чеської Республіки, із обов'язковим урахуванням національних культурно-історичних та соціально-економічних особливостей нашої держави.

Література

1. Діяльність уряду Чеської Республіки в напрямку інтеграції до НАТО. URL:http://osvita.ua/vnz/reports/world_history/4787. (дата звернення 06.03.2019).

2. Сайт Служби інформаційної безпеки Чехії: Розділ «Про нас». URL: https://www.bis.cz/o-nas. (дата звернення 06.03.2019).

3. Сайт Служби інформаційної безпеки Чехії: Розділ «Як працюємо». URL: https://www.bis.cz/jak-pracujeme. (дата звернення 06.03.2019).

4. Сайт Служби інформаційної безпеки Чехії: Річний звіт за 2017 рік. URL: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2017-vz-cz.pdf. (дата звернення 06.03.2019).

ЗМІСТ

УДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА УКРАЇНИ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ

АКТУАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

ПОГЛЯД НА ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ МОЛОДИХ ВЧЕНИХ І СТУДЕНТІВ.

Наукове видання

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

X Всеукраїнська науково-практична конференція

Збірник тез наукових доповідей
(Київ, 4 квітня 2019 року)

Електронне видання

Авторська редакція

Технічне редагування, макетування *Т. О. Коркач*

Формат 60x84/16. Ум. друк. арк. 20,23.
Обл.-вид. арк. 22,97. Тираж ___ прим. Зам. №

Видавець і виготовлювач
Національна академія Служби безпеки України,
вул. М. Максимовича, 22, Київ, 03022
факс: (044)257-30-35
E-mail: academy@ssu.gov.ua
Свідоцтво суб'єкта видавничої справи ДК № 99 від 23.06.2000