МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНА НАУКОВА УСТАНОВА
«ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ»

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

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

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

XII Всеукраїнська науково-практична конференція

Збірник тез наукових доповідей
(Київ, 26 березня 2021 року)

Електронне видання

Київ
2021

УДК 341.123(045)(0.034.2PDF)

Організаційний комітет конференції

Черняк С. М. – ректор Національної академії Служби безпеки України, доктор юридичних наук; ***Пилипчук В. Г.*** – директор Науково-дослідного інституту інформатики і права Національної академії правових наук України, доктор юридичних наук, професор, академік Національної академії правових наук України, академік Академії наук Вищої школи України, заслужений діяч науки і техніки України; ***Дашковська О. В.*** – науковий співробітник Державної наукової установи «Інститут модернізації змісту освіти» Міністерства освіти і науки України, кандидат хімічних наук, доцент; ***Мамченко С. М.*** – директор Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, доктор педагогічних наук, професор; ***Чорний Р. Л.*** – директор науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук, старший науковий співробітник; ***Гребенюк В. М.*** – заступник директора науково-організаційного центру Національної академії Служби безпеки України, доктор юридичних наук, старший дослідник; ***Давидова Т. О.*** – начальник організаційно-наукового відділу науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук

Рекомендовано до друку науково-організаційним центром
Національної академії Служби безпеки України
(протокол № 12 від 19 березня 2021 року)

Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). [Електронне видання]. – Київ : НА СБУ, 2021. – 346 с.

У збірнику тез висвітлюються актуальні проблеми розвитку системи інформаційної безпеки; захисту кібернетичної безпеки об’єктів критичної інфраструктури України, інші важливі питання, а також в окремій рубриці містяться погляди наукової молоді на зазначені проблеми.

Рекомендовано працівникам органів державної влади, науковцям, фахівцям із інформаційної та кібербезпеки, здобувачам вищої освіти, широкій громадськості.

Тези публікуються в авторській редакції. Організаційний комітет залишає за собою право не поділяти думку авторів.

УДК 341.123(045)(0.034.2PDF)

ВСТУПНЕ СЛОВО

Вітаємо учасників XII Всеукраїнської науково-практичної конференції **«Актуальні проблеми управління інформаційною безпекою держави»**, яку проводить Національна академія Служби безпеки України спільно з Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Інститутом модернізації змісту освіти Міністерства освіти і науки України.

Завдяки створеній науково-практичній платформі ми маємо можливість широкого обговорення актуальних проблем і шляхів забезпечення інформаційної безпеки та захисту інформаційного простору України, формування системи забезпечення кібербезпеки держави, удосконалення вітчизняного законодавства у сфері охорони державної таємниці та службової інформації, міжнародної взаємодії у сфері забезпечення інформаційної безпеки, удосконалення змісту вищої освіти фахівців з інформаційної безпеки держави та вироблення пропозицій щодо вирішення вкрай важливих для нашої країни проблем в умовах жорсткої інформаційної агресії Російської Федерації проти України, яка триває вже понад сім років.

Для зміцнення своїх позицій у Європі Російська Федерація застосовує «інформаційну зброю», намагається впливати на внутрішньополітичну ситуацію у європейських державах, підживлює тривалі конфлікти, які ж сама і створила. А для відновлення свого впливу в Україні Російська Федерація, продовжуючи гібридну війну, системно застосовує політичні, економічні, інформаційно-психологічні, кібер- і воєнні засоби. Її деструктивна пропаганда як ззовні, так і всередині України, використовуючи суспільні протиріччя, розпалює ворожнечу, провокує міжнаціональні та міжконфесійні конфлікти, підриває суспільну єдність.

У надзвичайно важких умовах протистояння гібридним загрозам, коли частина нашої території залишається тимчасово окупованою, Україна робить рішучі кроки у напрямку розвитку національного інформаційного простору та захисту свого інформаційного суверенітету, зокрема були реалізовані окремі положення вироблених попередньою конференцією рекомендацій: продовжує розвиватися нормативно-правове забезпечення національної безпеки в інформаційній сфері, вдосконалюється система підготовки фахівців з інформаційної та кібербезпеки, з підготовки й підвищення кваліфікації кадрів як державних, так і недержавних суб'єктів, з питань обміну інформацією щодо кіберінцидентів.

Указом Президента України від 14 вересня 2020 року № 392/2020 затверджена нова Стратегія національної безпеки України, у якій визначені ***поточні та прогнозовані загрози*** національній безпеці та національним інтересам України, зокрема:

- стрімко зростає роль інформаційних технологій у всіх сферах суспільного життя;

- розробляються системи озброєнь на основі нових фізичних принципів, із використанням квантових, інформаційних, космічних, гіперзвукових, біотехнологій, технологій у сфері штучного інтелекту тощо;

- сучасна модель глобалізації уможливлює поширення міжнародного тероризму та міжнародної злочинності у кіберпросторі;

- поширення коронавірусної хвороби (COVID-19) виявляє критичні проблеми в інформаційній та інших сферах, що загрожує національним інтересам та національній безпеці України.

Нова Стратегія національної безпеки України визначає також ***пріоритети національних інтересів України*** та національної безпеки і ***напрями забезпечення цих пріоритетів***.

З метою забезпечення цих пріоритетів *за напрямом посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі* на базі Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України створюється Науково-дослідний центр та нова Кафедра кібербезпеки, розробляються освітньо-професійні програми із спеціальності 125 Кібербезпека для підготовки фахівців за освітньо-кваліфікаційними рівнями бакалавр та магістр.

Стратегія національної безпеки України визначає ***пріоритетні завдання правоохоронним, спеціальним, розвідувальним та іншим державним органам*** відповідно до їх компетенції, зокрема – активна та ефективна протидія розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, російській та іншій підривній пропаганді. А ***основним завданням розвитку системи кібербезпеки*** вважається гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури в умовах сучасної цифрової трансформації.

Крім цього нова Стратегія національної безпеки України визначає ***завдання реформування й розвитку сектору безпеки і оборони***, зокрема – завершення створення національної системи кібербезпеки, формування сучасних спроможностей суб'єктів забезпечення кібербезпеки і кібероборони та зміцнення системи їх координації.

Тож ситуація, що склалася в державі, нові виклики та вимоги нормативно-правових актів вимагають від нас ще більших зусиль та наполегливої роботи щодо забезпечення національних інтересів та національної безпеки України в інформаційній та кіберсфері.

Розв'язання зазначених завдань вимагає конструктивних наукових дискусій та обміну набутим досвідом на цьогорічному науково-практичному форумі з метою напрацювання пропозицій щодо подальшого розвитку інформаційного суспільства, удосконалення системи забезпечення інформаційної та кібербезпеки України, захисту від агресивного інформаційного впливу з боку Російської Федерації.

З повагою,
організаційний комітет

ПРІОРИТЕТИ РОЗВИТКУ СИСТЕМИ ІНФОРМАЦІЙНОЇ І НАЦІОНАЛЬНОЇ БЕЗПЕКИ НА ПЕРІОД ДО 2030 РОКУ

УДК 351/354:78

Антипенко І.В.
кандидат юридичних наук,
Національна академія державного управління
при Президентові України

ПЕРСПЕКТИВНІ НАПРЯМИ ВПРОВАДЖЕННЯ НАЦІОНАЛЬНОЇ ОЦІНКИ ПОЛІТИЧНИХ РИЗИКІВ В УКРАЇНІ

Оцінка політичних ризиків, які викликані глобалізацією, є необхідною основою для вибору шляхів управління ними (приймати, уникати, пом'якшувати та/або передавати на інші рівні чи суб'єкти управління), а також побудови стійкості і готовності системи державного управління вчасно їх ідентифікувати і своєчасно реагувати на загрози, що постійно еволюціонують.

У сучасних реаліях України для моделювання оцінки стратегічних ризиків наразі має сенс частково апелювати до чинної Стратегії національної безпеки 2016 р. Немає сумніву, що у новій Стратегії на 2021–2026 рр. більшість нинішніх загроз продовжуватимуть еволюціонувати і далі. Утім фокусування на актуальній загрозі на середньострокову перспективу (п'ятирічку) як методичної одиниці позбавляє суб'єктів державного управління можливості відслідковувати їх еволюцію у динаміці та своєчасної оцінки виникаючих загроз. Такий підхід об'єктивно поступається кращим світовим кейсам проведення національної оцінки стратегічних ризиків, де в якості методичної одиниці розглядається сам ризик-ландшафт, котрим є кожен сегмент національної безпеки. В рамках кожного із них щорічно оцінюється вірогідність посилення/послаблення впливу як вже відомих ризиків, так і виникаючих (фактично оцінюється ступінь небезпеки кожного із них – їх трансформації у загрози). Оцінка ризиків на основі щорічного перегляду ризик-ландшафту по секторам національної безпеки є більш адаптивною моделлю, ніж вітчизняна. Результатом таких оцінок є складання матриць секторальних ризиків, на основі яких формується матриця загальнонаціональних ризиків. Тобто такий підхід відповідає стратегічному, а не реактивному підходу державного управління. Зв'язку із чим вважаємо методологічно виправданим застосування саме такого підходу до оцінки національних ризиків в Україні.

Внаслідок очевидності зростаючих впливів на внутрішню і зовнішню політику національних держав глобалізації і продукованих нею національних ризиків, для посилення спроможностей України захищати свої національні інтереси науково-практичний зміст отримує проведення в рамках загальнодержавної національної оцінки стратегічних ризиків та секторальної оцінки політичних, у тому числі, геополітичних ризиків із поміж аналізу загроз в інших секторах нацбезпеки. При цьому, оцінку останніх недоречно диференціювати від внутрішньополітичних ризиків. Це обумовлюється тим, що політичні ризики виникають, як внаслідок особливостей внутрішнього розвитку держави, так і являють собою продукт впливу зовнішнього середовища.

Придатність для потреб державного управління застосування методики ICRG для оцінки політичних країнових ризиків. У той же час, як було продемонстровано у національній оцінці стратегічних ризиків в системі ПВК/ФТ, даний індекс продуктивно комбінувати також із іншими міжнародними індексами політичної стабільності та крихкості держави, зокрема, The Political Instability Index, Political Stability Index, State Fragility Index, Failed States Index Scores та Political Stability and Absence of Violence.

Результати оцінки політичних ризиків пропонуємо відобразити у формі матриці національних ризиків. Оцінка і ранжування політичних ризиків пропонується по таким ризик-ландшафтам держави:

1. Політична система і система державного управління. Ризику політичної кризи має досліджуватись по таким критеріям: законодавча підтримка державної політики уряду; публічна підтримка політичного курсу впливовими внутрішніми і зовнішніми групами інтересу та громадськістю; зовнішній тиск на курс внутрішньої і зовнішньої політики в інтересах інших держав, у тому числі шляхом військової агресії, санкцій, ведення економічних війн, спотворення міжнародного іміджу, інформаційно-психологічних впливів, спрямованих на підрив соціальної і політичної стабільності, розвідувально-підривної діяльності та інших гібридних впливів; єдність у середині уряду при виробленні державної політики; фактор впливу тіньового лобізму і політичної корупції на вироблення державної політики; свобода діяльності політичної опозиції і політичних партій; забезпечення вільного волевиявлення; стабільність відносин основних політичних інституцій держави (президента, уряду, парламенту), а також вертикалі виконавчої влади і місцевого самоврядування; рівень підзвітності і прозорості органів публічного управління та менеджерів державних підприємств; вплив/наявність політичної нестабільності у прикордонних регіонах.
2. Соціально-економічні відносини і фінансово-бюджетна система.
3. Суспільні відносини.
4. Сектор безпеки і оборони.
5. Правоохоронна система.

Підкреслимо, що всі показники представлені у матриці, є тільки моделлю потенційної оцінки, оскільки повноцінний аналіз вимагатиме аналітичної роботи добре координованих експертних груп.

З аналізу вище наведених матеріалів зрозуміло, що національна оцінка стратегічних ризиків потребує відповідного інституційного забезпечення. В Україні на даний момент не створено чіткої структури правових норм і інституцій, що займаються стратегічним плануванням на урядовому рівні.

Зокрема, на інституційному рівні для проведення загальнонаціональної оцінки ризиків у контексті розбудови Системи управління національними ризиками (СУНР) доцільним є формування спеціальної міжвідомчої групи з проведення національної оцінки стратегічних ризиків при координації збоку головного суб'єкту СУНР, що має функціонувати при Головному ситуаційному центрі України.

Література

1. 10708/13 "Finalisation of the CCA Review Process: The EU Integrated Political Crisis Response (IPCR) Arrangements". Brussels: Council of the European Union, 24 June 2013. URL: http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2010708%202013%20INIT.

УДК 327.7:061.1

Арсенович Л.А.
Адміністрація Державної служби спеціального зв'язку
та захисту інформації України

ШЛЯХИ ФОРМУВАННЯ СИСТЕМИ ПІДГОТОВКИ КАДРІВ У СФЕРІ КІБЕРБЕЗПЕКИ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ В УМОВАХ РОЗВИТКУ ЦИФРОВОГО СУСПІЛЬСТВА УКРАЇНИ

Попри динамічне зростання ІТ-сектору, українські державні та приватні ІТ-підрозділи постійно стикаються з браком кваліфікованих та досвідчених фахівців з інформаційної безпеки, в тому числі й кібербезпеки. Як свідчать роботодавці, випускникам цієї спеціальності часто бракує спеціалізації чи практичних навичок. У свою чергу експерти у сфері кібербезпеки зазначають про негайну потребу у перегляді наявних освітніх програм та запровадженні більш сучасних підходів в навчанні, як для працівників державної, так і приватної кібербезпеки. Крім того, потребує вдосконалення й система підвищення кваліфікації фахівців із кібербезпеки, яка вимагає їх успішну адаптацію до професійної діяльності, а також постійний освітній контакт з професійною спільнотою на всій території країни.

У річному звіті Cisco за 2017 – 2018 роки з інформаційної безпеки вказується, що “миттєві атаки” стають усе складнішими, більш частими та тривалими. Більш третини кіберкомпаній, які були вражені хакерською атакою, понесли матеріальні збитки близько 20% прибутку. За даними спеціалістів “Лабораторії Касперського”, протягом року 30,01% комп’ютерів Інтернет-користувачів у світі хоча б один раз зазнавали веб-атаки класу Malware. Все це вказує на те, що потреба у фахівцях, які забезпечують захист інформаційних даних, буде зростати. Тому проблема підготовки справжніх професіоналів в області кібербезпеки є актуальною [1].

У цьому аспекті, надання послуг з навчання комп’ютерній грамотності, а також навчання щодо розроблення, модифікації, тестування та технічної підтримки програмного забезпечення можна забезпечити шляхом використання можливостей і потужностей віртуально-навчальних лабораторій, які на сьогодні активно впроваджуються “в життя” недержавними суб’єктами кібербезпеки, та введення яких у практичну площину стане дієвим розвитком всієї системи підготовки кадрів у сфері ІТ-технологій.

Основним завданням віртуальної лабораторії інформаційних технологій є моделювання процесів обробки даних у сучасних інформаційних системах та мережах. Програмною основою віртуальної лабораторії є технології хмарних обчислень, які доступні, у тому числі, у режимі віддаленого доступу через канали глобальної зв’язку, наприклад Інтернету [2].

Як відомо системні вимоги щодо розгортання хмарної інфраструктури передбачають використання двох комп’ютерів, один з яких виконуватиме функції сервера управління та первинного сховища, а інший відповідатиме за роботу віртуальних машин (гіпервізор) та містить вторинне сховище. Широкий спектр можливостей спеціального програмного забезпечення для віртуалізації надає унікальні можливості при організації навчального процесу, що і підтверджує доцільність та можливість його широкого використання як основного засобу формування системи знань, умінь та навичок при вивченні загальних і професійних цифрових компетенцій, ІТ-технологій та знань у сфері кібербезпеки, а також при формуванні системи умінь в галузі інформаційних технологій.

Серед переваг застосування віртуально-навчальної лабораторії для моделювання процесів у кібербезпеці для освітніх потреб державної і приватної кібербезпеки слід виділити:

у загальноосвітньому аспекті: формування фахових компетенцій, які можуть бути безпосередньо перенесені в реальність; підвищення якості самостійної навчально-пізнавальної діяльності; зацікавленість у вивченні матеріалу, розвиток мотиваційної діяльності; доступність та автоматизацію операцій; постійне удосконалення програмних систем та технологій тощо;

у організаційно-технічному аспекті: заощадження на придбанні апаратного забезпечення; доступ до комп’ютерів віртуально-навчальної лаборато-

рії можна забезпечити із традиційних та мобільних платформ, використовуючи стандартні протоколи (RDP, SSH, VNC); можливість використання різноманітних операційних систем; можливість використання потенційно-небезпечного програмного забезпечення без загрози ушкодження реальних комп'ютерів; можливість створення необхідних апаратних конфігурацій; можливість об'єднання віртуальних машин у локальну мережу та доступ до них засобами поширених протоколів; високу мобільність працівників та кібертренерів (викладачів), що вирішує питання "прив'язаності" до певного місця, а також створює можливості для самостійної роботи фахівців у сфері кібербезпеки.

Основними недоліками віртуально-навчальної лабораторії та хмарних технологій в цілому є: безпека інформації, постійне з'єднання з мережею Інтернет та можливість втрати даних у "хмарі".

Віртуальні освітні технології в світі тільки розпочали конкурувати з традиційними формами навчання, та в умовах сьогодення є безсумнівною підтримкою та стимулом до плідного навчання та цікавої наукової діяльності. Використання та подальше впровадження віртуально-навчальної лабораторії для моделювання процесів у кібербезпеці для потреб державної і приватної кібербезпеки стане ефективним інструментом навчання, який дозволить рухатися власною освітньою траєкторією, та розширить коло навчальних задач і збагатить їх сучасним змістом.

Література

1. Бурячок В. Л. Віртуальна лабораторія для моделювання процесів в інформаційній та кібербезпеці як засіб формування практичних навичок студентів / В. Л. Бурячок, С. М. Шевченко, П. М. Складанний // Кібербезпека: освіта, наука, техніка. - 2018. - № 2. - С. 98-104.

2. Олексюк В. П. Досвід організації віртуальних лабораторій на основі технологій хмарних обчислень / В. П. Олексюк // Інформаційні технології в освіті. - 2014. - Вип. 20. - С. 128-138.

УДК 340:351.86

Богуцький П.П.
доктор юридичних наук, доцент,
НДІ інформатики і права НАПрН України

САНКЦІЇ У СИСТЕМІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Система правового забезпечення національної безпеки України в інформаційній сфері засновується на загальних положеннях права інформаційної безпеки у структурі права національної безпеки України [1, с. 88-93] та

має свої особливі ознаки. Інформаційна безпека України (національна безпека в інформаційній сфері) у сучасних умовах є важливим чинником забезпечення національної безпеки, захисту національних інтересів України в інформаційному просторі. Необхідно визнати, що пріоритетні національні інтереси України в інформаційній сфері, на які зокрема вказує Доктрина інформаційної безпеки [2], наразі є досить вразливими для інформаційних атак, які здійснюються системно під час розв'язаної РФ війни. Такі дії мають не лише гібридні ознаки, але й характеризуються агресивністю, проведенням достатньо потужних інформаційних спецоперацій, де задіяні численні пропагандистські засоби й ресурси, які довершують вибудувану систему інформаційної агресії проти суверенітету, незалежності, територіальної цілісності України.

У системі правового забезпечення національної безпеки України в інформаційній сфері нормативно-правова складова узгоджується з інституційними механізмами, що відчутно демонструє їхню єдність. Особливе місце та призначення у цій системі займають санкції. Санкції (*лат. sanctio* – найсуворіша, непорушна постанова) у національному та міжнародному праві мають полісемічне значення, що підкреслює їх універсальність та дає можливість широко застосовувати у випадках порушення права, спричинення шкоди інтересам учасників правових комунікацій, де найбільш гострими є випадки спричинення шкоди національним інтересам.

Необхідно відрізняти санкції: 1) як міру та вид відповідальності, покарання, що визначені у нормі права у випадках вчинення правопорушення; 2) як засоби впливу (правового примусу) стосовно учасників правових комунікацій, діями яких порушуються публічні інтереси, права та свободи громадян, у тому числі у міжнародному праві; 3) як засоби управлінської діяльності щодо надання певних дозволів, прийняття рішень, у тому числі під час реалізації визначених законодавством процедур, процесуальних дій

В інформаційній сфері України держава з усією повнотою здійснює управлінську діяльність, у тому числі санкційну, забезпечуючи інформаційну безпеку як учасників інформаційних комунікацій, так і держави, суспільства загалом.

Найбільш суттєві порушення інформаційної безпеки знаходять свою реалізацію у спосіб встановлення санкцій у нормах права, а застосування – відповідно до рішення судів щодо притягнення до адміністративної або ж до кримінальної відповідальності у спосіб визначення у першому випадку – стягнень, у другому – покарання.

В інших випадках санкції виконують функцію обмежень у реалізації прав учасників міжнародних і внутрішніх правових відносин за певних, передбачених спеціальним законом обставин. Таким спеціальним законом в Україні є Закон «Про санкції» №1644-VII від 14 серпня 2014 року [3].

Зосередимо увагу на підставах застосування санкцій, на суб'єктах, стосовно яких поширюється дія закону, на видах санкцій.

Підставами застосування санкцій, як обмежувальних заходів, є: 1) вчинення дій, що: а) створюють загрози національним інтересам, національній безпеці, суверенітету і територіальній цілісності України (реальні, потенційні загрози); б) сприяють терористичній діяльності; в) порушують права і свободи людини і громадянина, інтереси суспільства та держави; г) призводять до окупації території; д) призводять до експропріації чи обмеження права власності, завдання майнових втрат; 2) створення певними діями перешкод: а) для сталого економічного розвитку; б) для повноцінного здійснення громадянами України належних їм прав і свобод; 3) резолюції, рішення, регламенти міжнародних органів (Генеральної Асамблеї та Ради Безпеки ООН, Ради Європейського Союзу відповідно); 4) факти порушень Загальної декларації прав людини, Статуту Організації Об'єднаних Націй.

Суб'єктами, стосовно яких можливим є застосування санкцій, спеціальний закон визначає: 1) іноземні держави; 2) іноземні юридичні чи фізичні особи; 3) інших суб'єктів. Однак загальною умовою для визначення вказаних суб'єктів є обов'язкова наявність підстави, тобто вчинення дій проти національних інтересів, національної безпеки України, порушень прав, свобод людина і громадянина та інших вказаних у законі дій або ж прийняття відповідних міжнародних актів. За таких обставин суб'єктами застосування державою санкцій є суб'єкти: 1) міжнародних відносин; 2) внутрішніх правових відносин, у тому числі юридичні, фізичні особи. Обов'язковою умовою для визначення суб'єктів застосування санкцій є наявність у їхніх діях визначеної законом підстави, про що зазначалось.

Види передбачених спеціальним законом санкцій є різними і стосуються економічної, у тому числі зовнішньоекономічної, господарської, фінансової тощо діяльності, користування об'єктами права власності, використання активів, у тому числі фінансових, здійснення і реалізації угод, переміщення капіталів, товарів тощо, здійснення заходів контролю, у тому числі щодо проведення фінансових операцій. Усі види санкцій можна розподілити на дві великі групи: 1) загальні санкції; 2) персональні санкції.

Повноваження щодо запровадження санкцій належать Раді національної безпеки і оборони України за зверненням Верховної Ради України, Президента України, Кабінету Міністрів України, Служби безпеки України з прийняттям відповідного рішення, яке затверджується Указом Президента та потребує ухвалення Постановою Верховної Ради України лише у випадку застосування загальних санкцій.

Законом не проведено диференціації, чіткого розмежування підстав та видів санкцій, які можуть бути застосовані до суб'єктів, які вчинили дії на шкоду національній безпеці України. Така юридична конструкція може ро-

зглядатися вразливою для застосування лише за умови порушення принципу верховенства права у рішенні РНБО України, коли пропорційність санкцій і порушень не витримуються, а також за умов відступу від принципів і норм міжнародного права, на яких засновується санкційний механізм захисту національних інтересів суверенних держав. В інших випадках загрози довільного, протиправного застосування санкцій відсутні.

Отже, у правових відносинах у сфері національної безпеки загалом та у сфері інформаційної безпеки зокрема держава має виключні повноваження стосовно захисту своїх суверенних прав, у тому числі у спосіб упровадження загальних і персональних санкцій.

Література

1. Богуцький П. П. Концептуальні засади права національної безпеки України: монографія. Київ-Одеса: Фенікс, 2020. 376 с.

2. 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/47/2017#Text (дата звернення 10.03.2021).

3.Про санкції: Закон України від 14.08.2014 р. №1644-VII. // База даних «Законодавство України»/ ВР України. URL: https://zakon.rada.gov.ua/laws/show/1644-18#Text (дата звернення 10.03.2021).

УДК 378+004.056

Богуш В.М.
кандидат технічних наук, доцент
Бровко В.Д.
кандидат технічних наук,
старший науковий співробітник
Мамченко С.М.
доктор педагогічних наук, професор,
Національна академія Служби безпеки України

ПІДГОТОВКА ФАХІВЦІВ З КІБЕРБЕЗПЕКИ В МЕЖАХ СПЕЦІАЛЬНОСТІ 256 НАЦІОНАЛЬНА БЕЗПЕКА (ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СФЕРІ ТА КІБЕРПРОСТОРІ)

Інформаційна сфера життєдіяльності людей знаходиться під впливом швидкого розвитку інформаційних технологій, коли формуються нові – віртуальні – середовища різноманітних просторів, які набувають все більшої значущості як у міжнародних та державних відносинах, так і у зовнішніх та внутрішніх відносинах конкретних організацій. До кола таких віртуальних

середовищ належить кіберпростір, що позначає особливу область соціальних взаємодій, опосередкованих сукупністю процесів, що відбуваються в інформаційно-комунікаційних мережах світу, і який перетворився на ще одне середовище буття та діяльності людини.

Уся інформаційна сфера у цілому та кіберпростір, зокрема, сьогодні являють собою життєве важливі галузі інформаційної, економічної, політичної, воєнної діяльності окремих людей, корпорацій, держав та їх спільнот, наднаціональних структур і утворень.

Майже відразу ж після свого виникнення кіберпростір перетворився у п'яте (після суші, моря, повітря і космосу) поле битви різних політичних і воєнних сил і залишається таким. Більше того, безліч протистоянь між розвідувальними організаціями різних країн, їх воєнними структурами, а також економічні та інформаційні війни, зокрема шпигунство і диверсії, розгортаються саме у кіберпросторі.

На сьогодні, в основну кількість спеціалістів з інформаційної та кібербезпеки готують у галузі знань 12 Інформаційні технології. Затверджений освітній стандарт для освітнього рівня бакалавр не врахував вимоги закону України «Про основні засади забезпечення кібербезпеки України» щодо створення національної системи кібербезпеки. Також потребує узгодження змісту стандарту з основними положеннями типового навчального плану з кібербезпеки, розробленого робочою групою консорціуму «Партнерство заради миру». Це значно звужує сферу його застосування – підготовка фахівців лише для забезпечення безпеки (захисту) кіберінфраструктури.

Для удосконалення системи підготовки фахівців і професіоналів із забезпечення національної безпеки в інформаційній сфері та кіберпросторі вважається доцільним використати введену у 2016 році спеціальність 256 Національна безпека (за окремими сферами забезпечення і видами діяльності). Пропонується провести уточнення та системний аналіз предметної області у сфері забезпечення кібербезпеки України, де предметна область – це частина реального світу, що розглядається в межах певного контексту – контексту національної безпеки.

Вимоги до результатів навчання, які є спільними для всіх можливих освітніх програм, у межах спеціальності стосовно забезпечення національної безпеки в інформаційній сфері та кіберпросторі дозволять закласти необхідні спеціальні компетентності.

Це дозволяє встановити додаткові обов'язкові результати навчання для освітніх програм, що передбачають надання певної професійної кваліфікації та/або спрямовані на підготовку фахівців для професій, для яких запроваджено додаткове регулювання.

У процесі розроблення профільної моделі компетентностей на бакалаврському рівні слід прийняти до уваги, що за аналогією з класичним визначенням інформаційної безпеки – під кібербезпекою фактично розуміють

властивість захищеності активів від загроз конфіденційності, цілісності, доступності, але в деяких абстрактних рамках – кіберпросторі (рис. 1).

Рис. 1. Взаємозв'язок понять безпека, простори інформаційний та кібернетичний

Що стосується власне забезпечення кібербезпеки, то в якості пріоритету доцільно виділити взаємодію між організаціями, що формують кіберпростір, автономні дії яких не забезпечують ефективний захист від кіберзагроз. Прикладна галузь кібербезпеки (рис. 2) є інтегрованою з поняттями інформаційної безпеки (ІБ), безпеки застосувань, мережної безпеки, безпеки глобальної мережі, а також безпеки критичної інформаційної інфраструктури.

Рис. 2. Прикладна галузь інформаційної та кібербезпеки

Виписаний загальний підхід дозволяє повною мірою здійснювати підготовку фахівців з кібербезпеки в межах спеціальності 256 Національна безпека (забезпечення національної безпеки в інформаційній сфері та кіберпросторі).

УДК 323:351.746.1
Ватраль А.В.
доктор юридичних наук,
Служба безпеки України

ДЕМОКРАТИЧНИЙ ЦИВІЛЬНИЙ КОНТРОЛЬ ЗА ДІЯЛЬНІСТЮ СПЕЦІАЛЬНИХ СЛУЖБ У КОНТЕКСТІ РОЗВИТКУ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Нині Україна перебуває на новітньому етапі історичного розвитку національної державності, що характеризується заснуванням та розбудовою сучасних демократичних інституцій, покликаних забезпечити передумови існування розвиненого громадянського суспільства та створити йому можливість безпосереднього доступу до здійснення державного управління. Прагнення України посісти належне місце в європейській системі колективної безпеки зобов'язує сприйняття національним сектором безпеки євроатлантичних цінностей та стандартів, а також механізмів їх імплементації. Євроатлантична культура безпеки – це певна філософія, набір цінностей, однією з яких є демократичний цивільний контроль за діяльністю спеціальних служб та заходами забезпечення національної безпеки. Тому, одним із пріоритетних завдань державної політики у сфері реформування й розвитку сектору безпеки і оборони, визначених Стратегією національної безпеки України, є зміцнення системи демократичного цивільного контролю [1].

Чинне законодавство передбачає, що демократичний цивільний контроль – це комплекс здійснюваних відповідно до Конституції і законів України правових, організаційних, інформаційних, кадрових та інших заходів для забезпечення верховенства права, законності, підзвітності, прозорості органів сектору безпеки і оборони та інших органів, діяльність яких пов'язана з обмеженням у визначених законом випадках прав і свобод людини, сприяння їх ефективній діяльності й виконанню покладених на них функцій, зміцненню національної безпеки України [2].

Спеціальні служби, під якими розуміють державні органи, уповноважені здійснювати розвідувальну та контррозвідувальну діяльність, забезпечувати внутрішню безпеку, безпеку інформації і системи управління державою, захищати національні інтереси тощо, є важливим елементом системи забезпечення національної безпеки будь-якої країни. Сучасні виклики і загрози національній безпеці України висувають перед спеціальними службами нові завдання, виконання яких може спричинити певні обмеження прав і свобод людини, а отже, посилюється необхідність підзвітності та

прозорості діяльності цих служб. На сьогодні до системи контролю за діяльністю спецслужб входять парламентський, Президентський та судовий контроль.

Досвід дієвого та професійного демократичного цивільного контролю за діяльністю спеціальних служб країн-членів НАТО свідчить про те, що обов'язкових євроатлантичних стандартів щодо організації такого контролю не існує. Кожна з держав у цій сфері керується національними інтересами, тенденціями розвитку геополітичної ситуації та виходить з форми державного правління. Правовою основою цивільного контролю за діяльністю спеціальних служб європейських країн є рекомендації ПАРЄ № 1402 (1999) «Контроль над внутрішніми службами безпеки у країнах-членах Ради Європи» та № 1713 (2005) «Про демократичний нагляд за сектором безпеки в країнах-членах Ради Європи», які не мають обов'язкового характеру. При реформуванні спеціальних служб України, досвід західних партнерів щодо створення системи демократичного цивільного контролю може стати корисним [3, с. 37].

Демократичний цивільний контроль за діяльністю спеціальних служб передбачає не лише виконання контролюючих функцій, а й співпрацю, діалог, взаємодію, спільний пошук способів вирішення проблем, готовність до порозуміння і бажання ефективно діяти. Важливо усвідомлювати, що дотримання розумного балансу між правом сили і силою права є одним із принципів демократії. Тому, створення системи демократичного цивільного контролю над спецслужбами є пріоритетним напрямом реформування сектору безпеки країни, яка стала на шлях демократичних перетворень [4, с. 442].

Очевидно, що ефективність демократичного цивільного контролю за діяльністю спеціальних служб багато в чому залежать від достатнього рівня обізнаності всіх його суб'єктів щодо сутності системи контролю, механізмів її впровадження з урахуванням національних особливостей, узгоджених з євроатлантичним баченням. Важливого значення тут набувають інформаційно-аналітичний супровід цього процесу та відповідне наукове забезпечення. Кваліфікована наукова й аналітична експертиза, урахування незалежної громадської думки мають базуватися на реальній взаємодії спеціальних служб із представниками Комітетів Верховної Ради України, Рахункової плати, Уповноваженим з прав людини, суддями тощо.

Отже, невід'ємною ознакою функціонування сектору безпеки і оборони у правовій державі є ефективно діючий інститут демократичного цивільного контролю за діяльністю спеціальних служб. У контексті розвитку системи забезпечення національної безпеки України цей інститут сприятиме формуванню позитивного мислення громадянського суспільства щодо функцій і повноважень спеціальних служб та розумінню необхідності впровадження в організацію їхньої діяльності європейських стандартів.

Література

1. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 р. № 392/2020 / Президент України. *Офіційний вісник Президента України*. 2020. № 19. С. 26. Ст. 926.

2. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII // Верховна Рада України. *Відомості Верховної Ради України.* 2018. № 31. Ст. 241.

3. Паливода В.О. Діяльність спеціальних служб іноземних держав у мінливому світі : збірник статей та аналіт. матер. Київ : НІСД, 2020. 336 с.

4. Власюк О.С. Національна безпека України: еволюція проблем внутрішньої політики : Вибр. наук. праці. К. : НІСД, 2016. 528 с.

УДК: 004.413.4

Вдовенко С.Г.
Національний університет оборони України
імені Івана Черняховського
Даник Ю.Г.
доктор технічних наук, професор,
Національний технічний університет України
«КПІ імені Ігоря Сікорського»

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ РАЦІОНАЛЬНОГО РОЗВИТКУ КІБЕРБЕЗПЕКИ І КІБЕРОБОРОНИ ДЕРЖАВИ

Штучний кіберпростір (КП) разом з природними (сухопутний, морський, повітряний, космічний) став сферою різноманітних конфліктів і можливих бойових дій. При цьому відбувається зміна традиційних форм і способів ведення протиборства. Гібридна війна (ГВ) є перманентним високотехнологічним конфліктом змінної інтенсивності, в якому комплекс дій (економічних, політичних, дипломатичних, інформаційних, психологічних, військових, кібер- й інших) призводить до системної дестабілізації та змін, корисних для досягнення інтересів вигодонабувача, в усіх сферах життя і діяльності держави, що є об’єктом агресії. Кібердії, після їх початку, не припиняються ніколи доки існуватиме КП.

Сучасна геополітика вимагає цілеспрямованої активної діяльності держав, щодо пошуку ефективної моделі оперативного управління кібербезпекою (КБ), підвищення ролі і значення державних інституцій щодо створення ефективної системи кібероборони (КО) та реалізації заходів з її забезпечення.

На сьогодні більшість держав світу відкрито або/та приховано провадять діяльність щодо: підвищення рівня функціональності національних систем КБ та КО; створення національних та коаліційних сил КО (кібервійськ,

кіберсил), визначення їх функцій, завдань, змісту діяльності, складу, порядку підготовки підрозділів, військових і цивільних фахівців; розробки стратегій, нормативно-правової бази; техніки для КО та тактики її застосування. В світі ще недостатньо з'ясовані масштаби та можливі наслідки застосування сил КО, які формуються, набувають оперативних спроможностей та вже вибірково застосовуються.

В доповіді розглядаються та обґрунтовуються принципи та особливості забезпечення раціонального розвитку КБ і КО держави. Виходячи з досвіду провідних країн світу побудову та розвиток системи КО доцільно здійснювати дотримуючись таких принципів: інтегрованість системи КО в багаторівневу систему КБ держави; безперервність функціонування системи КО; науково обґрунтовані законодавче, нормативно-правове, дефініційне супроводження; державно-приватне та міжнародне партнерство; узгодженість та взаємодія державних інституцій, суб'єктів КО держави, органів місцевого самоврядування, організацій, підприємств та установ різних відомств у сфері забезпечення КО держави; відповідність рівня всебічного забезпечення кіберсил – наявним та прогнозованим загрозам, ступеню економічного розвитку та рівню наукового-технічного потенціалу, з урахуванням воєнно-політичної обстановки та потреб оборони; керованість з єдиного координуючого органу з питань КО та забезпечення КБ; раціональність побудови сил КО; уніфікованість та випереджаючий розвиток систем підготовки військового й цивільного персоналу; однозначність критеріїв (індикаторів) загроз у сфері КО держави, рівня готовності систем КБ та КО, тощо.

Спираючись на перераховані принципи в провідних країнах світу (ПКС) сили КО та органи військового управління ними, утворюються, як правило в статусі окремого виду Збройних Сил (виключення – Ісландія, де збройні сили не передбачені конституцією, а функції забезпечення КБ покладені на національну поліцію) на базі існуючої військової інфраструктури, шляхом: об'єднання, реформування, перерозподілу функцій, перепідпорядкування військових частин, зміни напрямку діяльності, корегування наукової та освітньої діяльності наукових центрів та закладів освіти, включно утворення нових структурних підрозділів, закладів освіти, військових частин та підрозділів. Підрозділи радіоелектронної розвідки, радіоелектронної боротьби, інформаційно-психологічних операції, криптографічного забезпечення та криптологічної підтримки, геоінформаційного забезпечення, захисту інформації в інформаційно-телекомунікаційних системах – входять до складу та підпорядковані органам оперативного управління сил КО.

Наукове, науково-технічне, освітнє, навчально-тренувальне супроводження утворення системи КО здійснюється, як правило, багатофункціональними інтегрованими профільними військовими освітянсько-науково-до-

слідними закладами. Держзамовлення на підготовку фахівців, включно науково-педагогічних працівників – збільшується. При відсутності профільних ВНЗ – вони утворюються. Форми бойового застосування сил КО трансформуються до моделі застосування бойових команд під конкретне бойове завдання. Циклічність бойової підготовки залишається такою, що прийнята сьогодні.

ВИСНОВОК: Досвід ПКС щодо утворення та розгортання системи КО можливо й доцільно використовувати спираючись на вищеперераховані принципи, з урахуванням реальних військово-політичної обстановки, національних інтересів та законодавства України. Формування сил КО можливо здійснити шляхом комплексного та докорінного реформування сектору безпеки та оборони з оптимальним перерозподілом функцій, завдань, сил та засобів (СіЗ) і ресурсів, позбавлення їх невластивих функцій, використовуючи при цьому дані аналізу результатів аудиту нормативно-правового забезпечення, ефективності виконання визначених нормативно-правовими актами функцій, порівняння моделей інших держав.

Об’єднання у єдиній військово-організаційній структурі СіЗ, які діють в КП, створення раціональної системи управління ними на усіх рівнях від стратегічного до тактичного, завчасне формування вимог професійних стандартів до фахівців КО, визначення держзамовника та прогнозованих кількісних показників держзамовлення, формування профільного військового освітянсько-науково-дослідного закладу, матеріальне стимулювання фахівців, мають забезпечити утворення та розвиток раціональної системи КО держави.

УДК: 355/359.07

Войтко О.В.
кандидат військових наук
Солонніков В.Г.
доктор технічних наук, професор,
Національний університет оборони України
імені Івана Черняховського

ДЕРЖАВНА ІНФОРМАЦІЙНА ПОЛІТИКА ОСНОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Аналіз подій з початку загострення відносин між Україною та Російською Федерацією свідчить про неефективність інформаційної політики, нескоординованість діяльності різних суб’єктів забезпечення інформаційної безпеки держави, слабку присутність України в світовому інформаційному

просторі, тощо. В той же час проблеми забезпечення інформаційної безпеки держави та проведення дієвого комплексу заходів контрпропаганди, реалізації інформаційної політики, спрямованої на консолідацію українського суспільства та міжнародної спільноти з метою стримування збройної агресії, визначені вищим воєнно-політичним керівництвом України як найбільш пріоритетні. На спроможності України щодо адекватного реагування на виклики та ризики у воєнній сфері негативно впливають різні внутрішні та зовнішні фактори. Тому виникає потреба в розроблені системи поглядів та визначення задуму дій воєнно-політичного керівництва України, щодо реалізації державної інформаційної політики та забезпечення інформаційної безпеки України [1].

Головною проблемою реалізації державної інформаційної політики та забезпечення інформаційної безпеки України на мою думку є відсутність координації діяльності всіх державних інституцій в інформаційному просторі, конкуренція між ними, спрямованість значної частини інформаційних заходів на створення іміджу кожної інституції, а не на досягнення цілей держави. Не вирішення зазначеної проблеми приводить до неоднозначного розуміння державної інформаційної політики різними верствами населення України, населенням тимчасово окупованих територій, керівництвом та населенням країни-агресора РФ, міжнародної спільноти; дублювання функцій моніторингу інформаційного простору; неякісного та несвоєчасного виявлення, оцінювання та прогнозування наслідків загроз інформаційній безпеці України; ускладнення процесу обміну інформацією між різними державними інституціями.

Реалізація державної інформаційної політики України повинна здійснюватись з метою забезпечення єдиного розуміння офіційної позиції України, процесів та подій, які відбуваються в Україні різними цільовими аудиторіями, як в Україні, так і в світі; чіткого позиціонування України в світі; задоволення національних інтересів держави. В умовах конфлікту з РФ державна інформаційна політика України має бути спрямована на відновлення суверенітету та територіальної цілісності України, завершення конфлікту та стабілізації постконфліктної суспільно-політичної ситуації [2].

Для забезпечення інформаційної безпеки та створення відповідних умов необхідно визначити ряд основних завдань з реалізації державної інформаційної політики та забезпечення інформаційної безпеки України (в умовах конфлікту з РФ) таких як:

забезпечення постійного об’єктивного моніторингу інформаційного простору (внутрішнього та зовнішнього), систематичний аналіз результатів моніторингу;

чітке визначення єдиного загальнодержавного стратегічного наративу та особливостей його трактування різними державними інституціями України; створення механізмів унеможливлення відхилення від наративу при

здійсненні інформаційної діяльності різними державними інституціями;

скоординована діяльність в інформаційному просторі всіх державних інституцій України;

реалізація принципів та методології стратегічних комунікацій всіма державними інституціями, які здійснюють інформаційну діяльність;

виявлення, оцінювання та прогнозування наслідків загроз національним інтересам та національній безпеці України в інформаційній сфері;

протидія зовнішнім інформаційним впливам на населення України, зокрема на воєнно-політичне керівництво, особовий склад всіх складових Сектору безпеки і оборони України;

захист об'єктів критичної інформаційної інфраструктури України (зокрема від кібератак);

підвищення медіаграмотності населення України [3].

Реалізація запропонованих положень дозволить:

досягти єдиного розуміння сутності основних шляхів (способів) реалізації державної інформаційної політики та забезпечення інформаційної безпеки (в умовах конфлікту з РФ);

розробити теоретичну базу для вирішення проблеми реалізації державної інформаційної політики та забезпечення інформаційної безпеки (в умовах конфлікту з РФ) з єдиних концептуальних позицій;

створити дієву систему реалізації державної інформаційної політики та забезпечення інформаційної безпеки (в умовах конфлікту з РФ проти України, відновленню територіальної цілісності і державного суверенітету України, своєчасному виявленню і нейтралізації загроз національним інтересам та національній безпеці України в інформаційній сфері, задоволенню національних інтересів України в усіх сферах життєдіяльності держави.

Література

1. Указ президента України № 392/2020 14 вересня 2020 року "Про Стратегію національної безпеки України". URL: https://www.president.gov.ua/documents/3922020-35037.

2. Указ президента України № 555/2015 24 вересня 2015 року «Про нову редакцію Воєнної доктрини України». URL: https://zakon.rada.gov.ua/laws/show/555/2015#Text.

3. Войтко О.В. Реалізація державної інформаційної політики та забезпечення інформаційної безпеки в умовах конфлікту з Російською Федерацією. Періодичний науковий журнал "Грааль науки". 2021. – № 1 (лютий 2021). – С. 164-166. URL: https://doi.org/10.36074/grail-of-science.19.02.2021.

УДК 355.451
Горовий В.М.
доктор історичних наук, професор,
Національна академія Служби безпеки України

НАЦІОНАЛЬНІ СТРАТЕГІЧНІ КОМУНІКАЦІЇ У ВЗАЄМОДІЇ З ГЛОБАЛЬНИМ ІНФОРМАЦІЙНИМ ПРОСТОРОМ

В умовах становлення сучасного інформаційного суспільства все більш зростаючого значення набуває ефективне використання інформаційних ресурсів розвитку. У зв'язку з цим все більш важливим стає поряд із новим інфотворенням підвищення якості інформаційних обмінів через систему стратегічних інформаційних комунікацій в глобальному, загальносуспільному масштабі. На нинішньому етапі суспільного розвитку особлива увага до цих комунікацій пов'язана з тим, що :

- прогрес регіонів визначається параметрами світового науково-технічного прогресу, забезпеченням інформаційних обмінів, що сприяють впровадженню передових технологій у всьому спектрі напрямів сучасної людської діяльності;

- активізація участі в міжнародних науково-інформаційних обмінах, внесок до ресурсної основи глобального інформаційного простору нової інформації стає важливим критерієм визначення статусу кожної країни, нації в світовій ієрархії;

- процес управління інформацією розвитку, ефективним її використанням все більше пов'язується із вдосконаленням структури інформаційних комунікацій та формуванням визначального контенту стратегічних комунікацій для орієнтації національного інфотвореннння.

Інформаційні комунікації, насамперед стратегічні, стають ефективними механізмами керування інформаційними обмінами на сучасному етапі інформатизації. Адже саме вони забезпечують «скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків з громадськістю, військових зав'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави»[1].

Розвиток сучасної системи інформаційних комунікацій пов'язаний із процесом суспільної інформатизації, забезпеченням доступу до ресурсів розвитку і наявним уже соціальним структурам, і тим , що з'являються в результаті реалізації потреб трансформації соціальної системи сучасного

[1] Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України»: Указ Президента України № 555/2015 від 24.09.2015. https://zakon.rada.gov.ua/laws/show/555/2015#Text.

суспільства. Оскільки мова при цьому йде про розвиток інформаційної матриці національного інформаційного простору, то вдосконалення цієї системи, потребує сприяння держави в організаційно-правовій, матеріально-технологічній та безпековій сферах.

Стосовно проблеми трансформації системи соціальних комунікацій в сучасних умовах, то досить тривалий час побутувала думка про те, що така трансформація не має достатніх перспектив у зв'язку із принесеною глобалізацією загальною уніфікацією. Глобальні комунікації будуть все більше включати у зміст свого контенту все, що стосується суспільної еволюції. Цьому змісту у відповідності з основними інтересами глобалізаційного процесу мають підпорядкуватись національні, регіональні і всякі інші інтереси соціальних структур.

Однак практика сьогодення свідчить, що зростаюче число проблем, які постають перед цивілізацією на планетарному рівні, потребує оригінальних, різноманітних рішень різноманітного в своїй структурі суспільства. На постійні зміни в глобальних викликах не в змозі буде тривалий час реагувати уніфіковане суспільство. Такого роду проблеми знайдуть свій відгук, зокрема, і в економічній сфері, про що попереджують повідні економісти. У зв'язку з цим видається раціональним капіталізація національного та інших соціальних факторів розвитку в інтересах економічної діяльності, створення умов для використання їх потенціалу в рамках об'єктивного процесу глобалізації. Не випадково, у зв'язку з цим, Дж. Сорос вважає шкідливою надмірну уніфікацію для сучасних економічних процесів. Він, зауважує, що "надмірно покладатися на ринкові механізми доволі небезпечно... Самі по собі вони не здатні задовольняти колективні потреби, такі, як закон та порядок чи підтримка самого ринкового механізму. Неспроможні вони й гарантувати соціальну справедливість. Ці "суспільні товари" можна забезпечити лише за допомогою політичного процесу"[1].

Слід підкреслити, що в умовах розвитку інформаційного суспільства управління комунікативними процесами пов'язане насамперед із донесенням цільовій аудиторії переконливого, актуального і високоякісного контенту, що відповідає суспільно значимим орієнтирам. У зв'язку з цим зростає значення наукових установ, аналітичних центрів, інформаційно-аналітичних підрозділів бібліотечних та інших закладів, де концентрується інформаційний ресурс, засобів масової інформації, що відображають інтереси суспільного розвитку і відстоюють державницькі позиції в цьому процесі. В рамках національного інформаційного простору має ефективно функціонувати центр координації процесу забезпечення контентом стратегічних інформаційних комунікацій. Він має забезпечувати в інформаційних ресур-

[1] Джорж Сорос про глобалізацію. – Київ: Видавництво Соломії Павличко "Основи". – 2002. – С. 19–20.

сах цих комунікацій оптимальні співвідношення тенденцій загальносуспільного розвитку, відображати національні інтереси в країні і за рубежем, здійснювати нейтралізацію безпекових загроз в інформаційній сфері, бути конкурентоздатнім орієнтиром для розвитку всієї комунікативної системи суспільства.

УДК 327.5

Гребенюк А.В.
кандидат філологічних наук,
Національна академія Служби безпеки України

АНТИУКРАЇНСЬКА ПРОПАГАНДА: АКТУАЛЬНІ ПРОБЛЕМИ ВИЗНАЧЕННЯ ПОНЯТТЯ ТА РИСИ

Стратегія національної безпеки України, затверджена Указом Президента України № 392/2020 14 вересня 2020 року (далі – Стратегія), констатує (пункт 20), що деструктивна пропаганда як ззовні, так і всередині України, використовуючи суспільні протиріччя, розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність. Цей нормативно-правовий акт фактично визнав існування антиукраїнської пропаганди деструктивного характеру, нейтралізацію якої ускладнює відсутність цілісної інформаційної політики держави, слабкість системи стратегічних комунікацій.

У пункті 45 Стратегії зазначено, що державний суверенітет, територіальна цілісність, демократичний конституційний лад та інші життєво важливі національні інтереси України мають бути захищені від невоєнних загроз з боку Російської Федерації. На цьому тлі пріоритетними завданнями правоохоронних, спеціальних, розвідувальних та інших державних органів відповідно до їх компетенції передбачено: активну та ефективну протидію розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, російській та іншій підривній пропаганді [1].

На жаль, наведені норми не вміщають дефініцію пропаганди, що позначає одну із проблем – нормативну невизначеність цього явища.

Продовжуючи пошук, зазначимо, що Закон України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки» подає визначення пропаганди комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів [2]. Натомість, інші законодавчі акти не містять відповідних дефініцій взагалі.

У більшості лексикографіних джерел дублюються визначення пропаганди, розроблені за керівництва І. Білодіда та вміщені у Словнику української мови: поширення і постійне, глибоке та детальне роз’яснення яких-

небудь ідей, поглядів, знань; ідейний вплив на широкі маси або певні групи людей, що носить політичний або релігійний характер; система засобів масового поширення ідей, поглядів і т. ін.; складова частина назви певних відділів державних і громадських установ [3].

Розкриваючи певні процедурні етапи (поширення, роз'яснення ідей; чинення ідейного впливу) цього явища, окремі його риси (політичний чи релігійний характер впливу), ця дефініція все ж прямо не стосується антиукраїнської пропаганди, не окреслює її місця та ролі, методів і видів. У цьому полягає ще одна проблема – лексикографічна невизначеність поняття пропаганди.

Загальне розуміння пропаганди формують В. Петрик, А. Кузьменко, В. Остроухов, О. Штоквиш, В. Полевий, М. Дзюба, М. Галамба, І. Слюсарчук. На їх думку, це – поширення різних політичних, філософських, наукових, художніх, інших мистецьких ідей з метою їх упровадження у громадську думку та активізацію, тим самим використання цих ідей у масовій практичній діяльності населення [4].

Проте, у цьому визначенні знову ж окреслені суто процедурні особливості, які характеризують пропаганду в цілому, її загальну мету тощо. Натомість, вона не розглядається у прикладному аспекті, у пов'язаності з українськими реаліями.

Цікаво, що при цьому В. Остроухов розглядає пропаганду в одному спектрі серед методів спеціальних інформаційних операцій (далі – СІО) та актів зовнішньої інформаційної агресії (далі – АЗА): дезінформування, диверсифікації громадської думки, психологічного тиску, поширення чуток. Така локалізація позначає видову належність пропаганди.

Види СІО він поділяє на види: операції, спрямовані проти суб'єктів, які ухвалюють рішення; операції, спрямовані на компрометацію, завдання шкоди опонентам; операції, спрямовані на політичну (економічну) дестабілізацію. Отже, окрім політичної та релігійної спрямованості, передбачає економічний вимір пропаганди.

Цей учений конкретизує мету пропаганди, наголошуючи на її маніпулятивному характері, - здійснення вигідного впливу на громадську думку, провокування запрограмованих емоцій та зміни ставлення або поводження певної групи людей у напрямку, безпосередньо чи опосередковано вигідному організатору.

У цьому контексті актуальною залишається загроза національній безпеці України, визначена Законом України «Про основи національної безпеки України», що втратив чинність, в інформаційній сфері: намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [5]. Звідси, ще однією сферою (окрім політичної, економічної, релігійної), на яку впливає пропаганда, є інформаційна сфера.

Спектр сфер розширює визначення СІО – це проведення спецслужбами іноземних держав таємних операцій та акцій негативного чи навіть деструктивного ідеологічного, ідейно-політичного та соціального впливу на особу, групу осіб або суспільство в цілому з метою їх переорієнтації на інші цінності та ідеали, підштовхування до вчинення протиправних дій підриву й послаблення державного та суспільно-політичного устрою [4, с. 17].

СІО, частиною яких є пропаганда, проводяться шляхом поширення певної інформації різними способами, за допомогою використання комунікативних технологій з впливу на масову свідомість. Тобто, як СІО, так і пропаганда реалізуються за допомогою інструментарію соціальних комунікацій.

Зважаючи на викладене, до актуальних проблем визначення поняття антиукраїнської пропаганди належить його законодавча, лексикографічна й наукова нерозробленість. Це поняття за сучасних реалій потребує осучаснення, нового змістовного наповнення з урахуванням таких рис:

- пов'язаність зі спеціальними інформаційними операціями та актами зовнішньої інформаційної агресії проти України;
- належність до методів СІО та АЗА;
- видова належність до методів дезінформування, диверсифікації громадської думки, психологічного тиску, поширення чуток;
- реалізовуваність за допомогою інструментарію соціальних комунікацій;
- маніпулятивний характер;
- спрямованість на вплив в політичній, релігійній, економічній, соціальній, інформаційній сферах;
- потреба нейтралізації пропаганди за допомогою цілісної інформаційної політики держави, системи стратегічних комунікацій.

Література

1. Стратегія національної безпеки України, затверджена Указом Президента України № 392/2020 14 вересня 2020 року. URL.: https://www.president.gov.ua/documents/3922020-35037.

2. Закон України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки» від 9 квітня 2015 року № 317-VIII. URL.: https://zakon.rada.gov.ua/laws/show/317-19#Text.

3. Пропаганда. Словник української мови: в 11 тт. / АН УРСР. Інститут мовознавства; за ред. І. К. Білодіда. – К.: Наукова думка, 1970-1980. – Т. 7. – С. 246.

4. Петрик В.М., Кузьменко А.М., Остроухов В.В. та ін. Соціально-правові основи інформаційної безпеки : навч. посіб./За ред. В.В. Остроухова. – К.: Росава, 2007. – 496 с.

5. Закон України «Про основи національної безпеки України» URL.: https://zakon.rada.gov.ua/laws/show/964-15?find=1&text.

УДК 343.985:343.132:343.141
Грига М.А.
кандидат юридичних наук,
Національна академія внутрішніх справ

ОКРЕМІ ОСОБЛИВОСТІ ОГЛЯДУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

В умовах глобальної комп'ютеризації всіх сфер життєдіяльності огляд електронних документів, пошук віртуальних слідів, дослідження цифрових доказів стають традиційними слідчими діями, ефективне здійснення яких стає однією з умов успішного розслідування значної кількості злочинів.

Електронні документи наділені специфічними ознаками, які визначають особливості їхнього огляду. По-перше, електронний документ не є матеріальним об'єктом, а являє собою двійковий комп'ютерний код, що створений із застосуванням комп'ютерних засобів та існує на технічних носіях. Відсутність матеріального втілення зумовлює взаємозв'язок такого документа із його технічним носієм. Водночас, такий зв'язок не є нерозривним, оскільки документ може вільно переміщуватися в електронній мережі без технічного носія або існувати на кількох технічних носіях одночасно. Відтак електронний документ часто не можна дослідити без спеціального обладнання.

По-друге, електронні документи є більш «вразливими» доказами порівняно з традиційними, адже можуть бути легко знищені, а їхній зміст – змінений без видимих ознак. Крім того, аналіз слідчої практики засвідчує, що фахівці у сфері інформаційних технологій часто за завданням власника техніки інсталюють на комп'ютерні та мобільні пристрої спеціальні програмні продукти, які забезпечують автоматичне знищення інформації, що на них міститься, за умов неавторизованого чи неідентифікованого доступу [1, с. 65].

Особливості огляду електронних документів впливають також і на спосіб процесуальної фіксації результатів слідчої дії. Так, фізичні носії електронної інформації за потреби вилучаються, якщо ж електронні докази розміщені на серверах чи жорстких дисках підприємств, установ або організацій, слідчому рекомендується здійснити побайтову копію носія інформації. За допомогою спеціального обладнання відтворюється ідентична копія електронної інформації, яка знаходиться на технічному носії, після чого самі фізичні носії повертаються власникам. Аналогічні дії необхідно здійснювати, коли виникає необхідність в проведенні комп'ютерно-технічної експертизи [2, с. 82].

Вилучення комп'ютерного обладнання та периферійних мобільних пристроїв, у разі потреби, також потребує окремої уваги. Б. В. Черняховський пропонує детальний алгоритм дій у таких випадках: 1) зафіксувати ін-

формацію, яка відображається на моніторі та зберегти її; 2) перевірити налаштування BIOS і завантажити операційну систему з робочого примірника; 3) приєднати зовнішній носій інформації для копіювання значущої інформації (контрольний носій); 4) запустити програму запису зображення екрана монітора для додаткової фіксації процесу огляду, після чого створені в процесі огляду відеограму та зафіксовані зображення екрана монітора після завершення огляду зберегти на приєднаний зовнішній носій в окремому каталозі; 5) вивести на екран монітора інформацію про апаратне та програмне забезпечення комп'ютера, які його ідентифікують, зафіксувати її в протоколі огляду та зберегти на зовнішньому носії інформації в окремому файлі; 6) вивести на екран монітора налаштування мережевого адаптера, також зафіксувати; 7) створити файл-еталон для перевірки правильності підрахунку контрольних сум за допомогою призначеної для цього програми, перевірити та продемонструвати учасникам слідчої дії результати, після чого зберегти файл-еталон та файл із його контрольною сумою на носієві, призначеному для запису й зберігання доказової інформації; 8) провести детальний огляд інформації, що збережена на комп'ютері та акцентувати увагу учасників огляду (понятих) на її змісті та локалізації; 9) запустити браузер і ввести ідентифікаційні дані (доменне ім'я, паролі) віддаленого ресурсу, провести огляд зовнішнього інформаційного ресурсу (сайту), його наповнення; 10) за допомогою криміналістичного програмного забезпечення установити IP-адресу сайту, шляхи проходження в процесі обміну інформацією між сайтом і відповідним комп'ютером (для встановлення провайдера скористатися відповідним веб-ресурсом, що ідентифікує приналежність IP-адреси); 11) для кваліфікованого збереження (вилучення) виявленої інформації здійснювати побітове копіювання на під'єднаний спеціалістом зовнішній носій зберігання інформації, демонструючи ці дії понятим; 12) використовуючи криміналістичне програмне забезпечення, вивести на екран монітора інформацію про контрольну суму кожного файлу, значущого для слідства, що зафіксований на зовнішньому носії, зберегти її у відповідному окремому файлі; 13) після копіювання всієї виявленої значущої інформації підключити другий відформатований зовнішній носій зберігання інформації та скопіювати на нього всю інформацію з контрольного носія; 14) відключити контрольний та робочий носії із зібраною (збереженою) інформацією, вилучити диск з робочим примірником криміналістичного програмного забезпечення, здійснити пакування контрольного примірника носія з доказовою інформацією у спосіб, який унеможливить доступ до нього, опечатати й засвідчити на бирці з печаткою та підписами учасників слідчої дії, понятих; 15) зафіксувати порядок і зміст зазначених вище дій у протоколі огляду, обов'язково зазначивши контрольну суму інформації, зауваження, клопотання і доповнення від учасників слідчої дії [1, с. 64–65].

Відтак проведення огляду електронних документів, як часто значущого джерела доказів під час розслідування значної кількості злочинів, пов'язане з можливістю виникнення цілої низки ускладнень, зокрема: необхідність використання спеціальних знань в галузі ІТ-технологій та залучення відповідних спеціалістів; проблеми у доступі до необхідної інформації через використання злочинцями різного роду паролів, кодів та шифрувальних програм; втрата часу через процесуальні вимоги, пов'язані з отриманням дозволу на доступ до даних, розміщених у інтернет-провайдерів та ін.

Література

1. Черняховський Б. В. Особливості проведення слідчого огляду під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2020. 2(115). С. 58–68. doi: https://doi.org/10.33270/01201152.58.

2. Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони. Серія: Право.* 2017. № 4(58). С. 80–85.

УДК 316.485.6:351.746.1(477)

Давиденко М.О.
кандидат юридичних наук,
Національна академія Служби безпеки України

НАПРЯМИ ПРОТИДІЇ ПОШИРЕННЮ РЕЛІГІЙНОГО ЕКСТРЕМІЗМУ В ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Забезпечення стабільного існування та реалізації механізмів захисту внутрішньополітичної безпеки у релігійній сфері є одним із основних пріоритетів розвитку системи національної безпеки. На сьогодні актуальним є виявлення та попередження інформаційної деструктивної політики закордонних клерикальних центрів (далі – ЗКЦ), зокрема Російської Федерації, Угорщини, Польщі, Румунії та інших країн щодо України в умовах гібридної війни.

Відповідно до п. 33 Стратегії національної безпеки України «Безпека людини – безпека країни» Україна, прагнучи зміцнити заснований на демократичних нормах і цінностях міжнародний порядок, бере активну участь у протидії тероризму, політичному та релігійному екстремізму тощо. А у п. 46 вищезазначеної Стратегії одним із пріоритетних напрямів діяльності держави визначено протидію спробам розпалювання національної, расової чи релігійної ворожнечі та ненависті, приниження національної честі та гідності, образи почуттів громадян через їхні релігійні переконання тощо [1].

Дослідники погоджуються, що епоха інформаційного суспільства різко підвищила роль ЗМІ та мережі Інтернет у висвітленні процесів у релігійному середовищі України та визначили їх не тільки носіями і трансляторами, а й творцями інформаційної політики, зокрема і у релігійній сфері [2].

На сьогодні існує низка проблемних питань, що стосуються інформаційної агресії у релігійному середовищі:

1. Зростання числа ЗМІ, інтернет-сайтів, веб-порталів, блогів, інтернет-каналів, що належать закордонним клерикальним центрам, релігійним фундаменталістам, екстремістам і терористам.

2. Використання міжнародними терористичними організаціями і релігійно-екстремістськими об'єднаннями комунікаційних можливостей ЗМІ для поширення інформації щодо своєї діяльності, обґрунтування її законності і моральності, прямої чи прихованої пропаганди своїх ідей, а також забезпечення доступу широкого загалу (особливо молоді) до цих інформаційних ресурсів з метою популяризації радикальної релігійної ідеології.

3. Подання інформації за допомогою ЗМІ та мережі Інтернет щодо конкуруючих релігійних організацій часто має на меті створення новинного скандалу, поширення фейків та дипфейків, що може призводити до верифікації громадської думки, створенню атмосфери ненависті в суспільстві, радикалізації окремих вірян і груп, поширення релігійно- екстремістських настроїв.

Вищевикладене доводить, що з метою протидії поширенню релігійного екстремізму у інформаційному середовищі необхідно в повній мірі використовувати можливості ЗМІ та мережі Інтернет для висвітлення і демаскування справжніх цілей і прагнень організаторів і натхненників релігійного радикалізму та екстремізму, що реалізуються під ззовні привабливими гаслами боротьби за свободу, захист релігійних цінностей і національних інтересів.

Особливу увагу слід приділяти формуванню у громадян та вірян нашої багатонаціональної і поліконфесійної країни «інформаційний імунітет» до спроб залучити їх у релігійні конфлікти, поширити ідеології націоналізму, шовінізму, релігійної нетерпимості і ворожнечі. На наш погляд, важливим напрямком державної політики має стати система інформаційних та контрпропагандистських заходів із залученням ЗМІ та Інтернет-ресурсів щодо дискредитації в суспільстві релігійно-екстремістської ідеології, радикальної політики ЗКЦ, терористичних та екстремістських організацій. Так, ЗМІ і різні сайти в мережі Інтернет (особливо в соціальних мережах) можуть сприяти поширенню відомостей, які розкривають злочинну і антирадикальну сутність релігійних терористичних і екстремістських організацій.

Також, невід'ємною складовою реалізації Стратегії національної безпеки України «Безпека людини – безпека країни» є створення оновленого

медіа-середовища, в якому молодь могла б зосередитися на своїй ролі в якості миротворців, здатних реалізовувати свій професійний і творчий потенціал з метою запобігання виникненню та розвитку релігійно-екстремістських ідей і інших радикальних дій. Наприклад, йде мова щодо залучення молоді на радіо, телебаченні та Інтернет майданчиках для участі у відкритому і незалежному діалозі і дебатах щодо актуальних точок громадського і релігійного життя. Крім того, створення безпечного медіа-простору для відкритих і активних громадських дискусій із залученням політичних лідерів і місцевих національних і релігійних громад нами вбачається як найбільш ефективний засіб профілактики релігійного екстремізму у інформаційному середовищі України.

Література

1. Указ Президента України №392/2020 Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» / Електронний ресурс // [Джерело доступу]: https://www.president.gov.ua/documents/3922020-35037– Дата звернення 30.11.2020.
2. Протидія ксенофобії в Україні: законодавчі аспекти та адвокатська практика. Навчально-практичний посібник / колектив авторів. Київ, 2012 – 285 с.

УДК 37.02::355.232.6

Даник Ю.Г.
доктор технічних наук, професор,
Національний технічний університет України
«КПІ імені Ігоря Сікорського»

ОСОБЛИВОСТІ РАЦІОНАЛЬНОГО РОЗВИТКУ СИСТЕМИ ПІДГОТОВКИ ФАХІВЦІВ І НАУКОВИХ ДОСЛІДЖЕНЬ З ВИСОКОТЕХНОЛОГІЧНИХ ОБОРОННИХ НАПРЯМІВ ДЛЯ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ, ВКЛЮЧАЮЧИ ІНФОРМАЦІЙНУ ТА КІБЕРБЕЗПЕКУ

Національна безпека та оборона держави значним чином залежать від розвитку в ній високих оборонних технологій, зокрема, вирішення питань підготовки висококваліфікованих фахівців та проведення результативних наукових досліджень в цій сфері, організації та стану високотехнологічної складової військово-промислового комплексу. При цьому, складова військової освіти і науки є системоутворюючою і стратегічно визначаючою.

В своїх виступах секретар Ради національної безпеки і оборони (РНБО) України, на основі аналізу стану вищої освіти в Україні, проведеної фахівцями РНБО України та іншими провідними фахівцями в контексті нацбезпеки, неодноразово звертав увагу на кардинальну потребу в забезпеченні

відродження та розвитку в Україні системи підготовки сучасних висококваліфікованих фахівців, наукових і науково-педагогічних працівників з високотехнологічних оборонних напрямів, включаючи інформаційну та кібербезпеку.

Провідні країни світу – члени НАТО вирішенню зазначених питань, організаційному, науковому, кадровому та матеріально-технічному забезпеченню відповідних структур приділяють на теперішній час особливу увагу. В багатьох з них ефективність вирішення зазначених проблем досягається шляхом формування та забезпечення функціонування спеціалізованих інтегрованих освітньо-наукових комплексів (кластерів), військових університетів технологій, які здійснюють на єдиній базі освітню, наукову, дослідницьку і дослідницько-виробничу діяльність за високотехнологічними напрямами, що дає позитивний ефект в оптимізації витрат, якості і результативності підготовки висококваліфікованих фахівців та наукових досліджень [1].

Підготовка фахівців та наукові дослідження з цих питань в Україні здійснюються в достатньо великій кількості малопотужних профільних, а також у багатьох непрофільних освітньо-наукових та науково-дослідних закладах, що супроводжується дубляжем структур зі спорідненими напрямами та завданнями, збільшенням загальної чисельності управлінського і забезпечуючого особового складу, нераціональною витратою фінансових, матеріально-технічних і людських ресурсів та низькою якістю підготовки фахівців і наукових досліджень. Більше семи років держава знаходиться в стані гібридної війни, але ці питання, ключові в ній та прогнозованих конфліктах майбутнього, досі ефективно не вирішені, як стосовно забезпечення високоякісної підготовки нових фахівців так і збереження наявних високопрофесійних кадрів, а також здійснення, впровадження і ефективного застосування високотехнологічних розробок.

Успішне вирішення цих проблем можливе лише шляхом концентрації фахівців, ресурсів, всіх зусиль в одному місці у єдиному для сектору безпеки і оборони спеціалізованому освітньо-науковому закладі з високотехнологічних оборонних напрямів, які об’єднуються їх відношенням до інформаційного і кіберпросторів.

Виходячи з світового досвіду та з метою зниження ризиків та нейтралізації викликів і загроз, з якими зіткається Україна і які прогнозуються на майбутнє, зокрема, – в сфері воєнного будівництва і забезпечення сталого розвитку в Україні високотехнологічних оборонних напрямів є необхідність створення об’єднаного освітньо-наукового та дослідно-випробувального комплексу (кластеру) з високотехнологічних напрямів безпеки та оборони – Військового університету технологій, шляхом об’єднання існуючих військових освітніх і наукових структур з однотипними напрямами підготовки фахівців, наукових досліджень, інноваційної діяльності – для високотехнологічного забезпечення обороноздатності держави та раціонального використання фінансових, матеріально-технічних, кадрових та інших ресурсів.

Створення Військового університету технологій як інтегрованої загальнодержавної структури для комплексного проведення наукових досліджень, підготовки фахівців, наукових, науково-педагогічних кадрів, зосередження пріоритетних високотехнологічних напрямів з інформаційної та кібербезпеки, інформаційних технологій, технічних видів розвідки, радіоелектронної боротьби, технічного захисту інформації та криптології, космічних систем та геоінформаційного забезпечення, автоматизованої обробки інформації, інформаційно-аналітичної роботи, інформаційно-психологічних дій, оперативного управління силами та засобами, інформаційно-телекомунікаційних систем, військового і спеціального зв'язку, експлуатації та застосування робототехнічних комплексів і систем боротьби з ними, впровадження нанотехнологій у військовій сфері та зброї, побудованої на нетрадиційних і новітніх принципах, дозволить: запобігти дублювання однотипної підготовки фахівців та наукових досліджень різними міністерствами, відомствами та структурами держави; забезпечити раціональне використання фінансових, кадрових та інших ресурсів; підвищити якість підготовки фахівців з високотехнологічних напрямків для всіх видів збройних сил і інших міністерств і відомств сектора безпеки і оборони держави; суттєво підвищити ефективність здійснення досліджень, розробки, створення, випробування і застосування інноваційних високотехнологічних систем (зразків) озброєння і військової техніки.

Військові освіта і наука потребують проведення зазначених трансформацій для їх ефективної діяльності з метою забезпечення необхідного рівня обороноздатності держави в сучасних умовах та на перспективу.

Література

1. Бегма В., Шемаєв В. Розвиток технологій у провідних країнах світу. Уроки для України. *Українські технології асиметричного протиборства*. Київ : ІСД, 2020. С. 19-30.

УДК [94(470 + 571) : 355.014] : 94(477)

Даниленко В. М.
доктор історичних наук, професор,
Національна академія Служби безпеки України

ЗАГРОЗИ ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ У НАУКОВО-ОСВІТНЬОМУ ДИСКУРСІ РФ

Аксіомою стало твердження, що майбутній стан держави і суспільства визначають освіта і виховання підростаючого покоління. Зміцнення людського капіталу, зокрема, шляхом модернізації освіти і науки, – один із пріоритетів забезпечення національної безпеки України. Важливим напрямом реалізації цього пріоритету є здійснення гуманітарних заходів з деокупації

Криму й відновлення державного суверенітету на тимчасово окупованих територіях Донецької і Луганської областей.

Формування безпекового середовища значною мірою залежить від своєчасного виявлення загроз для національних інтересів України невоєнного характеру. До таких належать не тільки політична риторика потенційного противника, але й компетентності, які надаються в освітніх закладах країни-агресора, та світоглядні позиції, які прищеплюються його адептами. Для досягнення освітніх і навчальних цілей в Росії дуже вимогливо ставляться до кваліфікації авторів та змісту підручників і посібників з історії Росії й всесвітньої історії, інших суспільствознавчих дисциплін.

Щоб встановити причинно-наслідкові зв'язки і винести уроки з передумов гібридної війни РФ проти України, доцільно дослідити контент російської навчальної літератури, підготовленої протягом останніх десятиліть. Автори праць – науковці і педагоги – керувалися інтересами Російської Федерації і не зважали на те, якою може бути реакція в сусідніх країнах. Натомість українські науковці заради добросусідських відносин донедавна не привертали уваги суспільства до великодержавних амбіцій Росії, які набирали сил і активно впливали на думку громадськості. Індиферентні або й лояльні до путінського режиму російські діячі науки, освіти й культури сприяли поглибленню антиукраїнських настроїв у Росії. Такі явища нині ускладнюють припинення війни і повернення Україні територій, захоплених Росією.

Доцільно виділити фундаментальні особливості історичної освіти в Росії, що становлять потенційну загрозу для національної безпеки України.

У пострадянський період між Україною та Росією у сфері історичної науки і освіти накопичилися значні нерозв'язані проблеми. Вже після розпаду СРСР на сторінках офіційно затверджених міністерством освіти і науки РФ підручників відверто висловлювались територіальні претензії Росії до України, що зумовило нарощування чинників дестабілізації двосторонніх відносин.

Стосовно країн т. зв. «близького зарубіжжя» в Росії популяризувалась ідея формування поясу добросусідства по периметру російських кордонів. Яким способом і з якими наслідками цей пояс може бути створений яскраво показала політика РФ щодо Молдови, Грузії, України, Білорусі та низки країн, розташованих насправді далеко від новітньої російської імперії. Російські підручники з історії прагнуть переконати, що реалізація стратегії забезпечення національної безпеки – ключове завдання Росії, інтереси інших народів і світової спільноти – другорядні.

Здобувачам освіти на ментальному рівні вкарбовується думка про миролюбність і військову міць Росії, загрози від зближення України з ЄС і НАТО, неспроможність внутрішньої і зовнішньої політики України. З юних літ росіянам пояснюється, що на початку 2014 р. в Києві до влади прийшли

націоналісти, які запропонували скасувати закон про статус російської мови як регіональної. Це означало б «фактичну заборону використання російської мови», тому російськомовне населення в південних і східних районах України виступило «на захист своїх прав». У цих вихідних положеннях перекручено причини і наслідки, навіть не згадано про Революцію Гідності, про розв'язану Росією гібридну війну й агресію проти України.

Каноном освітнього процесу стало трактування окупації Росією Криму в рамках звернення В. Путіна до Федеральних зборів РФ 18 березня 2014 р. На викривленні історичної пам'яті й неправдивому твердженні, що «возз'єднання» Криму з Росією відбулося нібито на основі демократичних процедур і міжнародно-правових норм, формується історична свідомість підростаючого покоління. Зі шкільної лави росіянам прищеплюється думка, що Росії незмінно належить статус великої держави, яка просто зобов'язана впливати будь-якими засобами на світові процеси з метою формування стабільного, справедливого й демократичного світового правопорядку.

Події і факти, оціночні судження в навчально-методичній літературі подаються у найбільш вигідному для Росії світлі, в доступній формі і з видимістю об'єктивності шляхом дозування або приховування історичної інформації. Не даремно практично відразу після окупації українського Криму для місцевих закладів освіти терміново було підготовлено й надіслано нову історичну літературу. Викладені в навчальній літературі питання з історії України віддзеркалюють насамперед позицію російських політиків, а не новітню історичну думку. Мовний бар'єр, політичні та суб'єктивні чинники не дають змоги сучасним російським ученим враховувати здобутки української історіографії.

Нинішній науково-освітній дискурс РФ свідчить про наростаючу потенційну загрозу для національної безпеки України, дедалі більше затягування вузлів суперечностей і конфліктів у дво- та багатосторонніх відносинах. Росія намагається сформувати інтелектуальне підґрунтя нових посягань на територіальну цілісність і суверенітет України, підготувати модераторів військового й політичного тиску на Україну, ставлячи під сумнів ідентичність української нації та її право на самостійну незалежну державу.

В освітню політику Росії вмонтована система державної пропаганди, яка з великодержавних позицій завуальовує або ж виправдовує агресивні військові дії проти України, поглиблює духовний розкол і ворожнечу між російським і українським народами. Виходячи з цього, нагальними є потреби в контексті завдань забезпечення національної безпеки України посилити увагу до суспільствознавчих дисциплін, процесів формування історичної пам'яті й історичної свідомості на всіх рівнях освіти.

УДК 1:316.4
Дзьобань О.П.
доктор філософських наук, професор,
НДІ інформатики і права НАПрН України

КОНЦЕПТУАЛІЗАЦІЯ ПОНЯТТЯ «МЕРЕЖЕВА ВІЙНА» У ПРОБЛЕМНОМУ ПОЛІ ВІТЧИЗНЯНОГО БЕЗПЕКОЗНАВСТВА

Поняття мережевої війни – це новий якісний рівень розуміння цілей і завдань сучасної війни, збройних конфліктів. У сутнісному плані мережева війна зводиться до особливої форми ведення конфліктів, коли їх учасники застосовують мережеві форми організації, доктрини, стратегії та технології, максимально пристосовані до умов сучасного етапу розвитку інформаційного суспільства. Оскільки на даний час поняття «мережева віна» у вітчизняній науковій лексиці ще залишається певною соціально-політичною, соціально-економічною та культурною новацією, неологізмом, то виникає необхідність його концептуалізації.

У концепції мережевих війн основним поняттям є термін «мережа» – новий інформаційний простір, у якому і розгортаються основні стратегічні операції (війни) як розвідувального, так і воєнного характеру, а також відбувається їхнє медійне, дипломатичне, економічне, технічне та інше забезпечення.

Мережева війна здійснюється на основі інформаційно-комунікативних технологій (ІКТ), які заповнюють весь соціокультурний простір, пронизуючи відповідні соціально-політичні, соціально-економічні, культурні та ідеологічні процеси. Метою мережевої війни є досягнення абсолютного контролю над усіма учасниками історичного процесу у світовому масштабі. Мережева віна здійснює тотальне руйнування базових характеристик певної нації у всіх типах геополітичних просторів і здійснюється, як правило, у прихованій формі.

Бойові одиниці, система зв’язку, інформаційне забезпечення операції, формування громадської думки, дипломатичні кроки, соціальні процеси, розвідка і контррозвідка, етнопсихологія, релігійна і колективна психологія, економічне забезпечення, академічна наука, технічні інновації тощо – це все взаємозв’язані ланки єдиної мережі, між якими має здійснюватися постійний обмін інформацією. Головна мета – зібрати якнайбільше різноманітної інформації з різних джерел, а потім опрацьовуючи її за відповідним алгоритмом, прийняти рішення необхідні для перемоги. У мережевих війнах не є головною умовою безпосередня пряма окупація чи анексія території – достатньо встановити над нею мережевий контроль.

Характерними особливостями мережевої війни є: інформаційна сфера – така ж сфера бойових дій, як повітряно-космічний, морський і наземний

простір; асиметричний характер, тобто держава, що має невеликі збройні сили, може завдати серйозної шкоди державі, яка значно перевершує її за кількістю збройних сил; ведення мережевої війни безпосередньо або побічно впливає на події в реальному світі; мережеві війни суттєво впливають на когнітивні й емоційні процеси людей, на їх сприйнятливість і оцінку подій, на рішення, що приймаються; неясність і невизначеність правил застосування, відсутність повноцінних даних про можливості, швидкість та ефективність реакції радіоелектронних засобів і окремих елементів різних комп'ютерних систем; труднощі розпізнавання навмисних і ненавмисних (випадкових) дій і процесів у кіберпросторі; необхідність одночасного використання сил і засобів операцій як для впливу на супротивника, так і для захисту своїх збройних сил і сил союзників; відстань до цілі впливу не має значення; супротивник може наносити атаки анонімно і приховано; метою мережевої війни є забезпечення ефективності бойових дій в умовах мережевого управління військами тощо; успіх мережевої війни ґрунтується на методології використання інтегрованих можливостей усіх сил інформаційних операцій, сил їх забезпечення або пов'язаних з їх застосуванням.

Основною ідеєю мережевої війни є інформаційний вплив на людину і суспільство з метою управління та регулювання суспільних процесів у глобальному масштабі. Тому будь-яка мережева війна призводить до руйнування базових цінностей народу і держави, національної, конфесійної та культурної ідентичності; інформаційний та ідеологічний вакуум обмежує стратегічний вибір країни в глобалізованому світі і робить її частиною системи планетарного контролю. Фронт мережевої війни розташовується у ментальному просторі, де метою супротивника є руйнування традиційних базових цінностей даної нації і імплантація власних.

Мережева війна має два аспекти: технологічний і соціальний. Мережева війна у технологічному аспекті – це війна, в якій використовуються ІКТ, їх нові можливості. Мережа тут використовується як механізм. У цьому аспекті найбільш поширеними в сучасній мережевої комунікації є кібератаки на державні установи, оборонні та високотехнологічні компанії, а також економічні кіберзлочини з фінансовим збитком. У соціальному аспекті мережева війна характеризується формуванням нових груп, кібернайманців, які здійснюють напади – організовані групи хакерів з дуже високим рівнем підготовки, які можуть бути найняті урядами та приватними компаніями для організації і проведення складних ефективних цільових атак на державні структури та установи, приватні компанії з метою втручання в інформаційні бази даних, крадіжки інформації, знищення даних або інфраструктури тощо.

Отже мережева війна – це війна нового покоління, якісно новий рівень міждержавного протиборства та воєнного мистецтва, форма геополітич-

ного насильства з залученням великої кількості суб'єктів у комплекс різноманітних мереж, передусім інформаційних. Соціально-політична, соціально-економічна та культурна новація, в українській мові є неологізмом.

Як синоніми до мережевої війни часто застосовують поняття «мережецентрична війна», «інформаційно-центрична війна», «інформаційно-мережева війна», «гібридна війна», «електронна війна», однак кожне з наведених понять має свою специфіку і смислові особливості. Концепція мережевої війни у вигляді концепції мережецентричної війни покладена в основу воєнної доктрини США.

УДК 340.14

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

З ІСТОРІЇ РОСІЙСЬКО-ПОЛЬСЬКОГО ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА: ДОСВІД ДЛЯ УКРАЇНИ

Історія доводить, що методи інформаційного протиборства в кожну епоху мали важливе значення у забезпеченні досягнення деструктивних цілей тих чи інших держав. Особливо актуальними ставали і продовжують лишатися вони тоді, коли владний режим держави-агресора викликає ряд питань з точки зору легітимності та відповідності системі загальнолюдських цінностей. Якщо у стародавньому світі обман посідав чільне місце серед методів ведення бойових дій, то з часом він знайшов широке застосування і в мирну добу. На сьогодні в цьому плані привертає увагу відверто агресивна зовнішньополітична орієнтація Російської Федерації (далі – РФ), яка знаходить прояв у різних регіонах світу. Така ситуація більшою чи меншою мірою була характерною протягом усього періоду становлення російської державності, починаючи ще від Московського князівства. Усвідомлюючи порівняно невисокий рівень соціально-економічного розвитку своєї держави, російські правителі, тим не менш, повсякчас прагнули захопити якомога більше стратегічно важливих територій. Однією із них була і залишається Польща, і на її прикладі дуже яскраво видно технологію, котра застосовується Москвою для підкорення сильніших країн.

Загальновідомо, що остаточне входження польських територій до складу Російської імперії відбулося за наслідками поділів Речі Посполитої 1772, 1793 та 1795 рр. За рішенням Віденського конгресу 1815 р. було закріплено, що в її складі утворюється Царство Польське (в оригіналі – «Королівство Польське Конгресове»). Скориставшись ослабленням польської політичної верхівки в середині XVIII ст., російська влада ініціювала процес

ліквідації цієї держави, що потягнуло за собою встановлення там імперського, а потім і радянського впливу аж до 1989 р. У той же час, зацікавленість московських правителів у цих територіях була відомою ще задовго до названих подій. Так, факти обміну посольствами між цими країнами відомі мало не від проголошення в 1480 р. незалежності Московського князівства від Золотої Орди. Як зазначає класик української історичної науки М. Бантиш-Каменський, причинами встановлення давніх дипломатичних відносин між цими державами була їхня територіальна близькість, часте укладення двосторонніх угод і «взаємні потреби» [1, с. 75].

Перший підтверджений контакт між Королівством Польським та Московським князівством відносять до 1487 р. Саме того року посол короля Казимира IV князь Тимофій Володимирович Мосальський прибув до Москви зі скаргою на дії можайського князя Андрія Васильовича та князів Одоєвських. Проживаючи на прикордонних із польськими територіях, вони чинили на них набіги і поступово намагалися розширити межі своїх володінь. Тому польський король просив свого московського колегу вплинути на підданих, аби вони припинили такі недружні дії. Того ж року московський князь Іван III спрямував до Польщі посольство у відповідь під проводом боярина Михайла Кляпкіна Єропкіна. На нього покладалося завдання заперечити факти вторгнення на польські землі московських князів, а також висунути королеві у відповідь ряд територіальних претензій щодо колишніх давньоруських територій, щодо яких Москва заявляла своє правонаступництво.

Обмін посольствами такого плану залишався доволі характерним для московсько-польських взаємин аж до середини XVI ст., супроводжуючись введенням московських військ на польську територію. Перша помітна сутичка відбулася в 1514 р., що призвело до переходу Смоленська під московський контроль. У той же час, незважаючи на активні дипломатичні відносини, поляки не визнавали проголошеного того ж року титулу московського князя як царя, та притому «божою милістю». Гуртуючись із литовцями в єдину державу, що в результаті призвело до утворення Речі Посполитої в 1569 р., поляки мали на меті в тому числі посилитися задля протистояння московській агресії. Ігумен одного з литовських монастирів, сучасник подій, історик О. Магнус писав так: «Могутня країна – володіння великого князя Московського – займає велику площу, і було б добре, якби він задовольнявся цим, але з кожним днем він прагне розширити володіння і збільшити їх» [2, с. 64–65]. Більше того, уже на той час польські історики вдавалися до наукового пояснення різниці в походженні поляків і московітів. Серед найперших – Я. Длугош та М. Меховський, які на основі аналізу текстів Старого Заповіту Біблії стверджували, що польська та давньоруська народність походили від різних предків. Більше того, Я. Длугош взагалі виводив польське походження від бриттів та кельтів, що надалі стало основою

для наукових дискусій про віднесення поляків до західної або до східної гілки слов'янства [3, с. 22–23].

Надалі ці ідеї намагалися заперечити московські ідеологи, посилаючись на текст такого собі документу «Слово про погибель руської землі». Створення цього літописного уривка відносять до середини XIII ст., і зберігся він у формі вступу до новгородського літопису. Однак у тексті його є слова про те, що кордон руської землі проходив «од угрів до ляхів», у зв'язку з чим московіти заявляли свої права на польські землі. Апогеєм реалізації таких загарбницьких намірів став 1570 р., коли на підконтрольній на той час Речі Посполитій території Прибалтики, яка мала назву Лівонії, Іван IV Грозний проголосив маріонеткове царство під головуванням такого собі Магнуса. Надалі це сепаратне утворення мало бути використане для подальшого поширення впливу на Польщу та підкорення її території. Програш у Лівонській війні відтермінував реалізацію загарбницьких планів Москви, однак лише тимчасово.

Таким чином, застосовані в московсько-польському протистоянні кінця XV – середини XVI ст. ст. з боку Москви методи інформаційного протиборства спрямовувалися на поступову ліквідацію польської державності та перехід її територій під московський контроль. Заперечення фактів відкритої агресії щодо прикордонних територій, висунення територіальних претензій із викривленням історичної правди, створення фальсифікованих приводів з метою подальшого «захисту корінних російських територій» – це ті основні напрями московського деструктивного впливу, від яких потерпала середньовічна Польща і страждає сучасна Україна. Однак у першому випадку вони практично не давали бажаних результатів аж до ослаблення польської політичної еліти в середині XVIII ст. Сучасна ж тактика Кремля щодо створення маріонеткових сепаратистських утворень, направлення «іх там нєт» для допомоги в укріпленні злочинних еліт та поширення фальсифікованого викладу історії України сприяє продовженню тривалості режиму окупації на Сході України та в Криму. З огляду на сказане, залучення польського досвіду могло би суттєво сприяти прискоренню усунення відповідних загроз державній безпеці України.

Література

1. Бантыш-Каменский Н. Н. Обзор внешних сношений России (по 1800 год). Ч. 3 (Курляндия, Лифляндия, Эстляндия, Финляндия, Польша и Португалия). Москва: Типография Э. Лисснера и Ю. Романа, 1897. 319 с.

2. Савельева Е. А. Олаус Магнус и его «История северных народов». Ленинград: «Наука», 1983. 135 с.

3. Мыльников А. С. Картина славянского мира: взгляд из Восточной Европы: Этногенетические легенды, догадки, протогипотезы XVI – начала XVIII века. Санкт-Петербург: Центр «Петербургское Востоковедение», 1996. 320 с.

УДК 351.82
Іванова В.М.
кандидат економічних наук,
Національна академія державного управління
при Президентові України

ЗОВНІШНЬОЕКОНОМІЧНА БЕЗПЕКА: ОГЛЯД НАУКОВИХ ПІДХОДІВ

На даний час у вітчизняному науковому просторі немає єдиного визначення важливої складової економічної безпеки, а саме поняття «зовнішньоекономічної безпеки». Різні науковці надають безліч тлумачень, пропонуючи різні дефініції та намагаються віднайти найбільш вдалі формулювання. Здебільшого вітчизняні автори розходяться у поглядах на те, що зовнішньоекономічна безпека – це самодостатня наукова та прикладна категорія чи вона є складовою економічної безпеки держави загалом.

На думку, Мунтіяна В.І., зовнішньоекономічна безпека держави полягає у здатності забезпечувати всебічний динамічний розвиток національного господарства, нагальні потреби у критичному імпорті, сприятливі показники макроекономічних балансових агрегатів, перш за все загального платіжного балансу, бюджетного балансу, а також зовнішньоторговельного балансу в довгостроковій перспективі, що є передумовою стабільності національного валютного ринку, стійкості гривні [1].

Схоже визначення надають автори «Методичних рекомендацій щодо оцінки рівня економічної безпеки України», де зокрема зазначається, що «зовнішньоекономічна безпека полягає в спроможності держави протистояти впливу зовнішніх негативних чинників і мінімізувати заподіяні ними збитки, активно використовувати участь у світовому поділі праці для створення сприятливих умов розвитку експортного потенціалу і раціоналізації імпорту; забезпечувати відповідність зовнішньоторговельної діяльності національним економічним інтересам» [2].

Нормативно-правовою основою для наукових пошуків вітчизняних вчених є Методичні рекомендації щодо розрахунку рівня економічної безпеки України, затверджені наказом Міністерства економічного розвитку і торгівлі України від 29 жовтня 2013 року. В даному документі зовнішньоекономічна безпека є складовою економічної безпеки та визначається як стан відповідності зовнішньоекономічної діяльності національним економічним інтересам, що забезпечує мінімізацію збитків держави від дії негативних зовнішніх економічних чинників та створення сприятливих умов для розвитку економіки завдяки її активній участі у світовому розподілі праці [3].

На думку, Коковського Л.О., під зовнішньоекономічною безпекою країни розуміється інвестиційно-привабливий стан економіки країни, яка здатна генерувати конкурентоспроможну продукцію, забезпечуючи при цьому збалансованість зовнішньої торгівлі та стійкість фінансової системи країни в глобальній системі. Таким чином, зовнішньоекономічна безпека включає в себе такі складові: інвестиційну, зовнішньоторговельну та боргову [4]. В той же час зазначимо, що так само складовими зовнішньоекономічної безпеки є експортна та імпортна безпеки держави, а основні індикатори, що дозволяють розрахувати рівень зовнішньоекономічної безпеки визначаються як: відкритість економіки, коефіцієнт покриття експортом імпорту, питома вага провідної країни-партнера в загальному обсязі експорту товарів, питома вага провідної країни-партнера в загальному обсязі імпорту товарів, питома вага провідного товару в загальному обсязі експорту товарів, питома вага провідного товару за виключенням енергетичного імпорту в загальному обсязі імпорту товарів, питома вага сировинного та низького ступеня переробки експорту промисловості в загальному обсязі експорту товарів, частка імпорту у внутрішньому споживанні країни, індекс умов торгівлі, завантаженість транзитних потужностей нафтотранспортної системи, завантаженість транзитних потужностей газотранспортної системи.

Загалом зазначимо, що категорія зовнішньоекономічної безпеки, як невід'ємної складової національної безпеки, є досить складною та суперечливою, потребує вивчення та нового осмислення. Тому, в подальшому наукові пошуки будуть спрямовані на дослідження вказаних питань.

Література

1. Мунтіян В.І. Економічна безпека України Київ: КВІЦ, 1999. 462 с.

2. Методичні рекомендації щодо оцінки рівня економічної безпеки України / за ред. акад. НАН України С.І. Пирожкова. – Київ: НіпмБ, 2003. 42 с.

3. Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України: Наказ Міністерства економічного розвитку і торгівлі України від 29.10. 2013 № 1277. URL: https://zakon.rada.gov.ua/rada/show/v1277731-13#Text (дата звернення: 08.03.2021).

4. Коковський Л. О. Сучасні проблеми зовнішньоекономіної безпеки України та напрями їх подолання. Ефективна економіка. 2011. № 10. URL: http://www.economy.nayka.com.ua/?op=1&z=738 (дата звернення: 08.03.2021).

УДК 342:65.012.8(477)
Князєв С.О.
кандидат юридичних наук,
старший науковий співробітник,
Національна академія Служби безпеки України

УПОРЯДКУВАННЯ ЗАКОНОДАВЧОГО ВИЗНАЧЕННЯ ТЕРМІНА «ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ»

Серед різних видів інформації з обмеженим доступом найбільш уразливою для безпеки держави є безперечно державна таємниця. Тому не випадково, що для кожної країни світу охорона державної таємниці це важливе питання, ефективне вирішення якого потребує комплексного підходу. Правильне розуміння особливостей, спрямованості та реалізації заходів охорони державної таємниці, можливих перспектив подальшого їх застосування безперечно потребує системного підходу. Такий підхід, у тому числі, повинен передбачати дотримання єдності термінології, її несуперечливості й логічної впорядкованості.

Чітка й однозначна законодавча дефініція певного спеціального терміну або поняття мусить забезпечити його правильне розуміння і практичне використання, запобігти будь-яким хибним тлумаченням.

На теперішній час, «охорона державної таємниці» тлумачиться законодавцем як комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв.

З наведеного законодавчого визначення терміну «охорона державної таємниці» видно, що конструктивно він складається з двох частин: 1) комплекс заходів, з перерахуванням самих заходів; 2) спрямування цих заходів.

Так, з визначення терміну «охорона державної таємниці» зрозуміло, що ефективність охорони державної таємниці безпосередньо залежить від комплексного поєднання та застосування наступних чотирьох заходів: організаційно-правових; інженерно-технічних; криптографічних; оперативно-розшукових. Перелік основних організаційно-правових заходів наводиться у 18 статті Закону України «Про державну таємницю» і включає 8 заходів.

Інша стаття 36 цього ж Закону зазначає, що оперативно-розшукові заходи щодо охорони державної таємниці здійснюються відповідно до Закону України «Про оперативно-розшукову діяльність».

Зокрема, стаття 6 Закону України «Про оперативно-розшукову діяльність» серед підстав для проведення такої діяльності виділяє:

запити повноважних державних органів, установ та організацій про перевірку осіб у зв’язку з їх допуском до державної таємниці.

Разом з тим, 6 стаття Закону України «Про контррозвідувальну діяльність» серед підстав у контексті проведення такої діяльності, також визначає: вивчення і перевірку осіб, які оформлюються для допуску до державної таємниці.

Отже, котррозвідувальні заходи також повинні здійснюватись в межах охорони державної таємниці і, відповідно, бути відображені у терміні «охорона державної таємниці» поряд з іншими важливими заходами.

Крім того, не варто забувати й про контроль за забезпеченням охорони державної таємниці. Цьому питанню присвячена окрема 37 стаття Закону України «Про державну таємницю». Теж саме можна сказати й про важливість процедури віднесення інформації до державної таємниці, засекречування та розсекречування її матеріальних носіїв та її співвідношення з поняттям «охорона державної таємниці».

Саме тому виникає питання, що термін «охорона державної таємниці» у існуючий редакції не охоплює виключно всі важливі заходи які повинні або можуть увійти до вищезазначеного комплексу.

Повертаючись до другої частини терміну «охорона державної таємниці» - зазначимо, що вищеперераховані заходи спрямовані на запобігання:

- розголошенню секретної інформації;
- втратам її матеріальних носіїв.

Ці наслідки цілком слушно співвідносяться з протиправними діяннями передбаченими відповідними статтями Кримінального кодексу України (ст. 328; 329; 422).

Разом з тим, залишаються протиправні дії у сфері охорони державної таємниці, які формально можуть підпадати під інші статті Кримінального кодексу України й які, можна вважати, не врахованими у даному терміні, зокрема:

державна зрада, що полягає в умисних діяннях громадянина на шкоду, у тому числі, інформаційній безпеці [ст. 111];

шпигунство, тобто передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю [7, ст. 114].

Саме з метою протидії цим злочинам СБ України застосовує, у тому числі, оперативно-розшукові та контррозвідувальні заходи.

Звідти друга частина терміну «охорона державної таємниці» також не охоплює виключно всі важливі протиправні наслідки на попередження яких повинні бути спрямовані заходи охорони державної таємниці.

Зважаючи на викладене, з метою уникнення не правильного розуміння та подальшого використання терміну, вважається за доцільне здійснити його впорядкування за рахунок відходу від певної деталізації, що не дозволяє охопити та врахувати всі важливі складові, у наступній редакції: «охорона державної таємниці» - комплекс заходів, передбачених законодавством що забезпечують збереження державної таємниці та її правомірне використання.

УДК 351.1
Клименко О.М.
доктор юридичних наук, професор
Какауліна Л.М.
кандидат юридичних наук,
Інститут законодавства Верховної Ради України

ДО ПИТАННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ НАПРЯМКІВ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Тривале восьмирічне протистояння нашої держави воєнній агресії Російської Федерації продемонструвало застосування проти України, поряд із військовими збройними актами, численних технологій гібридної війни, що перетворило інформаційну сферу на ключову арену протиборства. За цей час України стикнулася із використанням проти неї найновіших інформаційних технологій впливу на свідомість громадян, які спрямовуються, зокрема, задля розпалювання національної і релігійної ворожнечі, поширюються пропагандистські заклики до зміни конституційного ладу насильницьким шляхом, порушення суверенітету та територіальної цілісності України.

Отже, загрози національній безпеці в інформаційній сфері, особливо в аспекті протидії руйнівному інформаційному впливу в умовах новітніх технологій гібридної війни, викликів глобалізації та вільного обігу інформації актуалізують потребу інноваційних підходів до формування системи захисту та розвитку інформаційного простору.

Формування системи інформаційної безпеки, яка б могла забезпечити виявлення, аналіз інформаційних загроз національній безпеці, а також протидію цим загрозам, убезпечити імідж держави на міжнародній арені є в числі пріоритетних завдань. Сьогодні зростає потреба у засобах накопичення, систематизації, зберігання, пошуку, передачі інформації, гарантування її безпеки, оскільки практично неможливо знайти площину соціальної активності, яка б не зазнала впливу інформаційних технологій: політика, право, економіка, медицина, освіта, культура, релігія тощо.

Про важливість забезпечення інформаційної безпеки наголошується в статті 17 Конституції України: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу».

Закріплене в Розділі І Основного Закону, яким окреслено коло загальних засад конституційного ладу, дане положення концентрує не лише політико-правовий вектор розвитку держави, а й сферу загальнонаціональних стратегічних інтересів, з якою пов’язують забезпечення конституційної моделі суспільно-державного устрою, демократичних цінностей та цілей розвитку.

Інформаційна безпека є складною, багатокомпонентною, динамічною, цілісною соціальною системою, складовими якої є підсистеми безпеки особистості, держави і суспільства.

Забезпечення інформаційної безпеки значною мірою сприяє досягненню успіху при вирішенні завдань у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності.

На основі рішення Ради національної безпеки і оборони України від 14 вересня 2020 р. Указом Президента України від 14 вересня 2020 р. № 392 було затверджено нову Стратегію національної безпеки України «Безпека людини – безпека країни». В її Розділі І визначаються пріоритети національних інтересів України та забезпечення національної безпеки, цілі та основні напрями державної політики у сфері національної безпеки, зокрема, пріоритетами національних інтересів України є відстоювання незалежності і державного суверенітету; відновлення територіальної цілісності у межах міжнародно визнаного державного кордону України; суспільний розвиток, насамперед розвиток людського капіталу; захист прав, свобод і законних інтересів громадян України; європейська і євроатлантична інтеграція. Одним з напрямів забезпечення вказаних пріоритетів є посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі та розвиток державно-приватного партнерства.

Поточні та прогнозовані загрози національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов окреслено у Розділі ІІ вказаної Стратегії. Зокрема, відмічається, що для відновлення свого впливу в Україні Російська Федерація, продовжуючи гібридну війну, системно застосовує політичні, економічні, інформаційно-психологічні, кібер- і воєнні засоби. Деструктивна пропаганда як ззовні, так і всередині України, використовуючи суспільні протиріччя, розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність. У цьому аспекті вказується на відсутність цілісної інформаційної політики держави, слабкість системи стратегічних комунікацій, що ускладнює нейтралізацію цієї загрози.

Основні напрями зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки містяться у Розділі ІІІ Стратегію національної безпеки України, серед яких слід акцентувати увагу на тому, що основне завдання розвитку системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації.

У Розділі ІV Стратегії висвітлено напрями та завдання реформування й розвитку сектору безпеки і оборони, зокрема, зміцнення бойового потенціалу Збройних Сил України, інших органів сил оборони; активізація вій-

ськово-технічного співробітництва з іноземними партнерами; реформування Національної поліції України з метою посилення кримінальної поліції та органів досудового розслідування; задекларовано зміцнення демократичного цивільного контролю за сектором безпеки і оборони України як запоруки законності та ефективності діяльності його складових тощо.

Комплексність завдань Стратегії втілено у заключних положеннях, якими передбачається розроблення додатково 14 стратегій і Національної розвідувальної програми, серед яких Стратегія забезпечення державної безпеки, Стратегія інформаційної безпеки, Стратегія кібербезпеки України тощо, проекти яких пропонувалося Кабінетові Міністрів України, державним органам за відповідними сферами національної безпеки подати у шестимісячний строк на розгляд Ради національної безпеки і оборони України, інформація про що на цей час відсутня.

В умовах гібридної війни Україна, яка стала об'єктом агресії, неминуче наражається на широкий спектр інформаційних загроз, нейтралізація яких вимагає вжиття надзвичайних правових і адміністративних заходів, з одного боку, а також може супроводжуватися істотним згортанням демократичних прав і свобод – з іншого боку. У цьому контексті слід наголосити на необхідності забезпечення балансу між інтересами національної безпеки й верховенством права, що є стратегічно важливим завданням держави.

В умовах деструктивного впливу мас-медіа країни-агресора не тільки на цільову аудиторію в Україні, а й в інших державах світу, збільшення кількості інтернет-ресурсів з терористичним забарвленням можна визначити низку основних напрямів вжиття заходів щодо захисту національного інформаційного простору та забезпечення національної системи інформаційної безпеки держави, серед яких удосконалення нормативно-правової бази у сфері інформаційної політики, яка б встановлювала взаємодію силових і правоохоронних структур з іншими державними органами, місцевим самоврядуванням та інститутами громадського суспільства, створення єдиного міжвідомчого координаційного органу, який би здійснював керівництво, координацію та контроль заходів інформаційної безпеки, наприклад у вигляді міжвідомчої комісії при РНБО, створити нову систему або посилити вплив Міністерства культури та інформаційної політики за здійсненням моніторингу популярних медіа ресурсів усіх видів, організувати грантові комплексні наукові дослідження у сфері інформаційної безпеки.

У рекомендаціях Національного інституту стратегічних досліджень «Залучення громадськості до вирішення питань цифровізації та кібербезпекової політики» зазначається, що формування ефективної національної системи кібербезпеки неможливе без залучення до цього всіх основних зацікавлених сторін – уповноважених державних органів, представників об'єктів критичної інфраструктури, науковців та громадського сектору. Саме наукова та експертна громадськість виявилась найменш включеною в

цю складову національної безпеки. З цією метою практичної реалізації положень статей 4 та 10 Закону України «Про національну безпеку України» доцільно розглянути можливість законодавчого закріплення вимоги до, щонайменше, основних суб'єктів національної системи кібербезпеки утворювати в своєму складі експертні ради (із законодавчо визначеною процедурою утворення, функціонування, повноваженнями тощо), які могли б виконувати функції з демократичного цивільного контролю у сфері кібербезпеки.

Література

1. Стратегія національної безпеки України «Безпека людини – безпека країни». Указ Президента України від 14 вересня 2020 р. №392/2020. URL: https://www.president.gov.ua/documents/3922020-35037.
2. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. URL: DOI https:// doi.org/10.32782/2524-0374/2020-2/52.
3. Бойко В.О. Залучення громадськості до вирішення питань цифровізації та кібербезпекової політики. URL: https://niss.gov.ua/sites/default/files/2020-10/kiberbezpekova-polityka.pdf.

УДК 004.056

Коваленко Є.В.
кандидат юридичних наук
Плетньов О.В.
кандидат юридичних наук,
Інститут підготовки юридичних кадрів для СБУ
Національного юридичного університету ім. Я. Мудрого

ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА ДЕРЖАВИ ЯК ОБ'ЄКТ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Стрімкий розвиток цифрових технологій та нові реалії соціальних відносин, що призвели до активізації суспільно значущих процесів у різних галузях життя, спричинили зростання популярності цифрової (електронної) комунікації, у межах якої створення, зберігання, оброблення та передача інформації виконуються технічними засобами, зокрема за допомогою глобальної комп'ютерної інформаційної мережі Інтернет. Завдяки майже новим технічним можливостям «всесвітня павутина» стала не лише джерелом інформації, а й певної небезпеки.

У цих умовах головним завданням держави є вжиття заходів, що дозволять сприяти розвитку електронних комунікацій, протистояти протиправним діям у кіберпросторі, уникнути або зменшити негативні наслідки від реалізації кіберзагроз - наявних та потенційно можливих явищ і чинників, що загрожують кібербезпеці.

Серед чинників – уразливість інформаційної інфраструктури держави. Так, за останній час дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які забезпечують безпеку, оборону, захист від надзвичайних ситуацій, а також сервери їх офіційних Інтернет-представництв і електронної пошти. Стрімке збільшення кількості кібератак на державні інформаційні ресурси свідчить про посилення хакерської діяльності, яка має на порушення роботи інформаційно-телекомунікаційних систем державних органів. Таку діяльність можуть здійснювати: транснаціональні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій хакери-одинаки, кіберзлочинці, іноземні державні органи, терористичні та екстремістські угруповання, транснаціональні корпорації та фінансово-промислові групи тощо. При цьому загроза використання кібернетичних засобів існує як з середини країни, так і з-за кордону. Крім того, реальною є загроза використання телекомунікаційних можливостей української інформаційної інфраструктури в якості «проксі-платформи» для приховування атаки на інформаційну інфраструктуру іншої держави.

На сьогодні можливі факти проведення кібератак є малопрогнозованими, проте їх результатом є, зазвичай, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування інформаційно-телекомунікаційних систем, які безпосередньо впливають на стан національної безпеки і оборони. Відтак існуючі загрози вимагають впровадження комплексних заходів, спрямованих на забезпечення кібербезпеки.

Зазначимо, що незадовільний стан захисту інформації, який фіксується при проведенні заходів державного контролю, стає потенційною загрозою, що може призвести до порушення сталого функціонування об'єктів критичної інфраструктури, і як наслідок, до зниження обороноздатності країни, її економічної, фінансової і політичної нестабільності, послаблення іміджу та інвестиційної привабливості тощо.

Забезпечення необхідного рівня інформаційної безпеки об'єктів критичної інформаційної інфраструктури має бути засновано на використанні єдиних вимог захисту інформації від несанкціонованого доступу або зміни, дії деструктивних інформаційних впливів, а також сертифікованих засобів попередження і виявлення інформаційних небезпек та захисту інформації, що постачаються підприємствами, які отримали в установленому порядку необхідні ліцензії (дозволи). Для реалізації комплексного підходу щодо забезпечення інформаційної безпеки необхідне чітке виконання положень Концепції створення державної системи захисту критичної інфраструктури України [1].

При цьому, як зазначає ст. 1 Стратегія кібербезпеки України, забезпечення кібербезпеки України «досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, має базуватися

на принципах: верховенства права і поваги до прав та свобод людини і громадянина» [2].

Отже, основним підходом у напрямку формування державної політики у сфері кібербезпеки та кіберзахисту має бути формування узгодженої з міжнародними стандартами нормативно-правової бази та вдосконалення законодавства у сфері захисту інформації та забезпечення безпеки об'єктів інформаційної інфраструктури держави від загроз у кіберпросторі. Це вимагає від суб'єктів забезпечення кібербезпеки (до яких відноситься і Служба безпеки України) вжиття узгоджених заходів і впровадження комплексних підходів державних органів у співробітництві з приватним сектором та громадянським суспільством, без якого неможливо вирішити питання забезпечення захищеності інформаційної інфраструктури держави.

Література

1. Концепція створення державної системи захисту критичної інфраструктури: Схвалено розпорядженням КМУ від 06.12.2017 № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017 (дата звернення: 06.03.2021).

2. Стратегія кібербезпеки України: Затверджено Указом Президента України від 15.03.2016 № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 06.03.2021).

УДК [004.02/.032/.421] + 621.391 +004.031.42+007.2

Козубцов І.М.
кандидат технічних наук, професор РАЕ
Козубцова Л.М.
кандидат технічних наук,
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут

ПРОГНОЗ МОЖЛИВИХ НАСЛІДКІВ НАСТАННЯ «КОЛАПСУ ІНФОРМАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ»

Проблема виникла в результаті бажання автоматизувати і дистанційно управляти, контролювати технологічними і виробничими процесами привели до створення "Автоматизованої системи управління технологічними процесами" (АСУ ТП) та інформаційні системи спеціального призначення (ІС СП). Легкий доступ з Інтернету до компонентів АСУ ТП (ІС СП) спонукає мотиваційний інтерес у хакерів до пошуку вразливостей для проведення кібернетичних атак.

Дійсне дослідження є продовження дослідження з попереднього опису "Майбутнє безпекове середовище 2030, а саме обґрунтовано поняття терміну глобального колапсу інформаційно-телекомунікаційних систем [1] та

розглянуто найбільш типові механізм створення штучного глобального колапсу інформаційно-телекомунікаційних систем (ІТС) [2].

Висвітлити прогноз можливих наслідків в результаті настання "Колапсу ІС СП".

В даний час існує безліч видів і інструментів дії на ІС СП та мережі і АСУ в мирний час [3]. При цьому кібернетичні атаки цивільного характеру (не на військові об'єкти) загрожують державній і міжнародній безпеці, коли вони проводяться у військово-політичних цілях. Перелік найбільш вразливих об'єктів інфраструктури та вірогідні наслідків вразі їх порушення функціонування у вигляді руйнування інфраструктур техногенних катастроф і людських жертв, представлені в табл. 1.

Таблиця 1

Перелік вразливих ОКІ та ймовірні наслідки
в разі їх порушення функціонування

Сфера	Об'єкти інфраструктури	Наслідки
Промислові об'єкти	Атомні електростанції	Аварії із-за виходу з під контролю центрифуг із збагачення урану
	Нафтопереробні заводи	Аварії, викиду отруйних речовин
	Газопровід	Вибух на газових сховищах
	Енергетичні комплекси	Вихід зі строю або знищення системи енергозбереження населених пунктів
	Телекомунікаційні системи	Вихід зі строю або порушення системи зв'язку, порушення роботи пристроїв у мережі
Залізничні сполучення	Швидкісні поїзда Автоматизовані вокзали Автоматизовані залізничних станції	Людські жертви із-за зупинки або виходу із робочого стану поїзда, що рухається на високій швидкості.
Інтелектуальні системи	Адміністративні будинки, промислові підприємства, аеропорт, банк, офіс, готель, спортивні споруди, лікарня	Вимкнення освітлення, ліфтів, блокування роботи будівель, тощо.
Інформаційні системи світового значення	Електронні науково-технічні бібліотеки, електронні енциклопедії за аналогом "Wikipedia"	Порушення процесу збереження та спотворення важливої наукової та історичної інформації. Порушення обміну науковою інформації, створення, поширення, використання, зберігання і знищення інформації, порушення її цілісності та конфіденційності. Розповсюдження, та використання хибної інформації.

Інформаційні системи спеціального призначення	АРМ; бази даних; підсистеми підтримки прийняття рішень, озброєння	Неконтрольований початок бойових дій в результаті деструктивного інформаційного впливу на автоматизовану систему управління в результаті хибного результаті одержаного з підсистеми підтримки прийняття рішень щодо застосування озброєння
Системи соціального значення	Державні інформаційні агентства (…/gov.ua), ЗМІ, бездротовий зв'язок, Веб-сайти, E-mail	Суспільний колапс. Можливі маніпуляції суспільною думкою. Викривлення подій в людському сприянні. Реалізація психологічного тиску на суспільство для підготовки та ведення гібридної війни.
	Соціальні мережі спілкування Facebook, Telegram messages, Instagram , viber та ін.	

Наслідки воєнного характеру можуть настати в разі колапсу ІС СП (воєнного) призначення, можливий збій та несанкціоноване керування військами та озброєнням до прикладу, як у науково-фантастичному фільмі "Terminator", де штучний інтелект мережі "SkyNet" отримавши доступ до керування системою протиракетною оборони та ядерним озброєнням Збройних сил США створив умови до знищення людства. І хоча на перший погляд це виглядає фантастично, але сьогоднішні "кібервійни" та "кіберпростір" з науково-фантастичного роману У. Гибсона "Нейромант" (1982) перекочували в сучасну реальність. Військові США запропонували розглядати кіберпростір як п'ятий театр військових дій (поряд з наземним, морським, повітряним і космічним).

Бажання автоматизувати з можливістю дистанційно управляти, контролювати стан озброєння та Збройними силами шляхом створення АСУ та ІС СП наразі в Україні немає такої можливості. І мабуть це добре, оскільки втрата такого керування у випадку несанкціонованого доступу до системи управління могло б призвести до повного колапсу воєнного характеру планетарного значення. Цьому всіляко сприяють "здоровий глузд" і розуміння тієї небезпеки, в разі створення АСУВ на елементній базі інформаційно-телекомунікаційних систем іноземного виробництва та на транспортних мережах власниками, яких є іноземні громадяни.

Література

1. Козубцов І.М., Куцаєв В.В., Козубцова Л.М., Терещенко Т.П., Штонда Р.М, Черноног О.О. Обґрунтування поняття терміну глобального колапсу інформаційно-телекомунікаційних систем / Міжнародна науково-практична конференція "Застосування

інформаційних технологій у підготовці та діяльності сил охорони правопорядку" (15.03.2019). Х.: НАНГ України, 2019. С. 57 – 59.

2. Козубцов І.М., Куцаєв В.В., Козубцова Л.М., Терещенко Т.П. Кібернетичні атаки як механізм створення штучного глобального колапсу інформаційно-телекомунікаційних систем / Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). К.: НА СБУ, 2019. С.221 – 223.

3. Михайлов Д.М., Жуков И.Ю., Шеремет И.А. Защита автоматизированных систем от информационно-технологических воздействий. М.: НИЯУ МИФИ, 2014. 184 с.

УДК 004.056

Козюра В.Д.
кандидат технічних наук, доцент,
Національна академія Служби безпеки України
Хорошко В.О.
доктор технічних наук, професор,
Національний авіаційний університет

ПРОБЛЕМИ УПРАВЛІННЯ УРАЗЛИВОСТЯМИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Практично в будь-якій сучасній ІТС існують помилки в програмному забезпеченні і недоліки апаратної структури, що не дозволяє на 100% забезпечити безпеку і захищеність. Ці недоліки, утворюють уразливості, через які порушники і здійснюють свої кібератаки.

Уразливість (vulnerability) – це недолік в системі кібербезпеки ІТС (її апаратної і програмної компоненти), використовуючи який порушник може навмисно порушити цілісність, доступність, конфіденційність ІТС і призвести до її неправильної роботи.

Уразливості є результатами помилок програмування, недоліків, допущених при проектуванні системи, використання ненадійних паролів, шкідливих програм, скриптів і SQL-ін'єкцій. Деякі уразливості мають відомі експлойти. Поширені типи вразливостей включають в себе:

- порушення безпеки доступу до пам'яті (переповнення буфера);
- помилки перевірки введених даних (невірна підтримка інтерпретації метасимволів командної оболонки, SQL-ін'єкції, ін'єкції коду, ін'єкції електронної пошти, обхід каталогів, міжсайтовий скриптинг в веб-застосуваннях, міжсайтовий скриптинг при наявності SQL-ін'єкції);
- стан гонки (помилки часу-перевірки-до-часу-використання, гонки символьних посилань);
- помилки плутанини привілеїв (підробка міжсайтових запитів в веб-застосуваннях);

- ескалація привілеїв (підривні атаки);

- вразливості zero-day.

Перед службою кібербезпеки ІТС стоїть досить складне завдання створення ефективної стратегії управління уразливостями, що дозволяє своєчасно їх виявляти та усувати, перш ніж порушники зможуть скористатися цими недоліками.

У стратегія управління уразливостями можна виділити наступні стадії.

1. Інвентаризація ресурсів – усі пристрої системи, програмне забезпечення та інформаційні ресурси повинні бути зареєстровані і ці списки повинні постійно перебувати в актуальному стані. Відсутність інвентаризації ресурсів може привести до недостатнього виділення або перевитрати коштів на забезпечення безпеки.

Інструменти: Asset Center (HP), LANDesk Management Suite, StillSecure, Enterprise від компанії Foundstone Enterprise

2. Контроль інформації, що надходить в організацію. Найбільш важливим є інтернет-трафік, що надходить з мережі організації. Збільшилася кількість шкідливих програм, від яких потрібно захищатися. Слід звернути увагу на цей інформаційний потік, щоб не допустити проникнення загроз з мережі. Управління інформацією також стосується даних організації. Якщо до конфіденційної інформації отримають доступ порушники, це може завдати непоправної шкоди. У службі кібербезпеки повинна бути створена команда з реагування на інциденти для обробки всього, що загрожує збереженню і передачі інформації. Крім цієї команди, організація повинна прийняти політику найменших привілеїв щодо доступу до інформації. У стратегії управління необхідно передбачити створення механізмів виявлення та запобігання доступу порушників до файлових систем. Ці механізми впроваджуються в мережу і на пристроях кінцевих користувачів, щоб заборонити вхід шкідливому трафіку і гарантувати надходження сповіщень про наявність підозрілих дій, таких як відстеження (snooping).

Інструменти: Координаційний центр CERT, Security Focus, Symantec Security Response.

3. Оцінка ризиків - перш ніж ризики можуть бути нейтралізовані, команда із забезпечення безпеки повинна провести поглиблений аналіз вразливостей, з якими вона стикається. Організація повинна розставити пріоритети одних вразливостей над іншими і виділити ресурси для їх усунення. Оцінка ризиків включає наступні етапи:

- визначення області дії (об’єкт захисту, його чутливість і рівень, на якому його потрібно захищати);

- збір даних про існуючі політики та процедури, які застосовуються для захисту організації від кіберзагроз;

- аналіз політик і процедур - стане відомо, чи достатньо їх в організації для усунення вразливостей, а також аналіз вразливостей. Фахівці, які проводять тестування на проникнення, повинні імітувати реальні атаки і виявляти системи і пристрої, які відчувають стрес і піддаються компрометації в процесі цього. В кінці виявлені вразливості класифікуються відповідно до ризиків, які вони представляють для організації;

- аналіз загроз (дій, кодів, програмного забезпечення, які можуть привести до підробки, знищення даних або переривання функціонування служб) для оцінки ризиків, які можуть виникнути в організації;

- аналіз прийнятних ризиків - існуючі політики, процедури та механізми безпеки спочатку оцінюються, щоб визначити, чи є вони адекватними. Якщо вони такими не є, передбачається, що в організації є уразливості. Робляться коригувальні дії для забезпечення їх поновлення та апгрейда, до тих пір поки вони не стануть достатніми.

Найбільша проблема на цьому етапі управління уразливостями - відсутність повної інформації.

Інструменти: ArcSight Enterprise Security Manager.

4. Оцінка вразливостей - включає в себе виявлення вразливих ресурсів. Ця фаза проводиться за допомогою ряду узгоджених спроб злому і тестів на проникнення. Об'єктами цих атак є сервери, принтери, робочі станції, брандмауери, маршрутизатори і комутатори в мережі організації. Мета полягає в тому, щоб змоделювати реальний сценарій злому з використанням тих же інструментів і методів, які може використовувати потенційний порушник. Мета даного етапу - не тільки виявити вразливості, але і зробити це швидко і точно.

Інструменти: Nessus, NMap, Harris STAT, Foundscan Foundstone, Zenmap.

5. Складання звітів і відстеження виправлень помилок. Звіти допомагають адміністраторам зрозуміти поточний стан безпеки в організації та області, де вона все ще вразлива, і вказують на це відповідальній особі. Звіти також дають керівництву щось відчутне, щоб у нього була можливість зв'язати це з майбутнім управлінням організацією.

Виправлення запускає реальний процес завершення циклу управління уразливостями. Всі вразливі вузли, сервери та мережеве обладнання відслідковуються, після чого приймаються необхідні заходи для усунення вразливостей, а також захисту їх від подальших експлойтів. Це найважливіше завдання в стратегії управління уразливостями, і якщо воно виконане належним чином, управління уразливостями вважається успішним. Операції, які виконуються в цьому завданні, включають в себе визначення відсутніх виправлень і перевірку на предмет наявності доступних оновлень для всіх систем організації.

На даному етапі зустрічається безліч проблем, оскільки саме тут визначаються рішення для всіх вразливостей:

1) звіти не покривають всі необхідні сфери і не містять всієї необхідної інформації про ризики, з якими стикається організація (погано складений звіт може привести до слабких заходів щодо виправлення загроз);

2) поганий зв'язок між постачальниками програмного забезпечення і організацією може викликати проблеми, коли необхідно виконати виправлення системи;

3) процес виправлення може бути поставлений під загрозу через відсутність співпраці кінцевих користувачів.

Інструменти: Enterprise Manager (Foundstone), інструмент звітності від компанії Latis.

6. Планування реагування - важливий крок у стратегії управління уразливостями. Він не представляє проблем, тому що вся важка робота була пророблена на попередніх етапах. Це важливо, тому що без нього організація як і раніше стикатиметься із загрозами. На цьому етапі важлива тільки швидкість виконання.

УДК 355.40

Комаров В.С.
доктор військових наук, старший науковий співробітник
Олексіюк В.В.
кандидат військових наук
Балик І.В.
Військова частина А1906

УДОСКОНАЛЕННЯ РОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ ЯК СКЛАДОВОЇ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Сучасний світ характеризується глобальними економічними, геополітичними та геокультурними змінами, прискореним технологічним прогресом, але, разом з тим, і більш витонченим застосуванням воєнної сили, як засобу одностороннього вирішення ключових проблем світової політики, та відповідною зміною викликів і загроз у сфері воєнної безпеки. У цьому контексті особливо актуальним стає передбачення можливих причин виникнення і реалізації загроз воєнній безпеці України, як складовій національної безпеки держави, для їх своєчасного попередження, виявлення та нейтралізації. Тому питання визначення шляхів удосконалення розвідувальної діяльності в сучасних умовах є вкрай важливим та актуальним завданням.

У сучасних умовах воєнній розвідці належить важлива роль. Це пов'язано з тим, що розвідувальний орган Міністерства оборони України

здійснює діяльність у воєнній сфері, сфері оборони, військового будівництва, військово-технічній сфері та кібербезпеки [1], здійснює інформаційно-аналітичне забезпечення підготовки та застосування ЗС України, а також є суб'єктом системи стратегічних комунікацій і здійснює розвідувальне забезпечення проведення інформаційних заходів [2; 3].

Виявлений рівень та характер загроз у воєнній сфері суттєво впливають на оснащення, чисельність, структуру та підготовку Збройних Сил, і значною мірою визначають масштаби, характер, а також темпи трансформаційних процесів у сфері оборони. Крім того, прогнозування можливих загроз та причин виникнення конфліктних ситуацій стає головним підґрунтям визначення ролі, місця та основних завдань власне воєнної розвідки в процесі забезпечення воєнної безпеки України. Отже, роль та місце воєнної розвідки в забезпеченні воєнної безпеки, як складової національної безпеки держави, а також як безпосереднього суб'єкта бойових дій, має нині вирішальне значення.

У доповіді пропонується підхід для реалізації цього завдання. Виходячи із потреб забезпечення воєнної безпеки держави, процесу системної трансформації Збройних Сил України, зокрема, з огляду на імплементацію стандартів НАТО, розвідувальну діяльність доцільно удосконалювати за такими основними напрямами: оптимізація розподілу завдань за рівнями та відповідними сферами [1], визначення їх пріоритетності та забезпечення виконання відповідними силами і засобами розвідки; пошук нових форм і способів виконання визначених завдань; обґрунтування раціональних за складом і структурою органів розвідки з погляду максимально ефективного виконання ними завдань; оптимізація системи управління розвідувальною діяльністю; удосконалення всебічного забезпечення розвідувальної діяльності; розробка та впровадження у практику розвідувальної діяльності сучасного науково-методичного апарату організації планування та застосування відповідних сил і засобів; розвиток новітніх технічних засобів розвідки.

Отже, практична реалізація визначених вище напрямів удосконалення системи розвідувальної діяльності дасть змогу наростити можливості з добування інформації, що збільшить її обсяг і підвищить достовірність, необхідну для виконання завдань оцінювання обстановки.

Збільшення обсягу та підвищення якості потрібної інформації стане основою для створення єдиного розвідувально-інформаційного простору, що забезпечить ефективне виявлення ознак можливих змін обстановки й своєчасне інформування відповідних суб'єктів про загрози воєнній безпеці державі з метою їх нейтралізації.

Література

1. Закон України "Про розвідку". Zakon.rada.gov.ua/912-IX (дата звернення 10.03.2021).

2. Доктрина зі стратегічних комунікацій / Військова керівна публікація військовим організаційним структурам з порядку реалізації стратегічних комунікацій у Збройних Силах України. Затверджена Головнокомандувачем Збройних Сил України 12.10.2020 р.К. : Апарат Головнокомандувача ЗС України, 2020. - 34с.

3. Наказ Міністра оборони України від 22.11.2017 р. № 612 “Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України”.

УДК 352/354

Корж І. Ф.
доктор юридичних наук,
старший науковий співробітник,
НДІ інформатики і права НАПрН України

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В СУЧАСНИХ УМОВАХ

В сучасних умовах гібридного протистояння у світі, механізми забезпечення безпеки мають бути адекватними – такими ж гібридними, як і гібридні загрози. Це – аксіома нинішнього життя, і не лише нинішнього. Доцільно згадати другу світову війну, в якій одні країни вели бойові дії відповідно до міжнародного гуманітарного права (право війни, право збройних конфліктів) [1,2,3], а інші нехтували ним; аналогічно бойові дії у В’єтнамі, Афганістані, Югославії, Сирії, події в Криму і на Сході України тощо. Нехтування загальновизнаними міжнародними правилами вирішення кризових ситуацій – характерна ознака поведінки багатьох країн сучасності.

Інформаційні засоби ведення сучасної війни в багатьох випадках теж не відповідають положенням загальновизнаних правил поведінки суб’єктів міжнародного права. Необхідно зазначити, що згадані засоби застосовуються не лише в сугубо інформаційній сфері, а й активно використовуються в інших – духовній, моральній, соціальній, культурній, освітянській, історичній, науковій тощо сферах. Тим самим сучасна інформаційна війна зі своїми спеціальними інформаційними операціями є комплексною, як і саме інформаційне право – яке є комплексним, міжгалузевим правом. Як і комплексне інформаційне право, яке регулює інформаційні відносини в різних сферах життєдіяльності, засоби боротьби і протидії в інформаційній війні чи інформаційному протистоянні, як зазначалося вище, теж застосовуються у різних сферах. І державна влада має враховувати зазначене при здійсненні протидії агресору, і відповідно діяти, застосовуючи належні для цього механізми і засоби, включаючи і гібридні.

Так, інформаційні загрози в історичній сфері, які, насамперед, виходять від Російської Федерації, яка прагне подати історію у вигідному для

себе форматі і в негативному для України, потребують активного залучення Національної академії наук України для розвінчування замовних Кремлем і перекручених ним історичних подій. І зазначений підхід є дуже важливим, оскільки на сьогоднішній день не можна стверджувати про активне використання українською владою у згаданому протистоянні з Кремлем представників української історичної та правничої науки.

Багато вже років Українське суспільство знаходиться на зламі духовного стану, внаслідок активної антиукраїнської політики Російської православної церкви та її сателіта в Україні – Московського патріархату, якою ведеться фактично підривна діяльність проти незалежності нашої держави, про що свідчать значна кількість фактів такої діяльності. Державній владі необхідно невідкладно залучити фахівців і практиків у даній сфері, які займають патріотичну позицію, для напрацювання теоретико-методологічних та практичних підходів до вдосконалення системи забезпечення духовної безпеки суспільства, розроблення моделі державного регулювання процесу забезпечення духовної безпеки з метою ідентифікації та нейтралізації загроз в релігійній сфері суспільного життя. Однак, на сьогодні влада фактично дистанціювалася від вирішення даної проблеми.

На наше переконання, потребують більш рішучих кроків щодо забезпечення безпеки з боку державної влади у сферах освіти і культури, в яких продовжується ведення Російською Федерацією інформаційно-психологічної війни, здійснення приниження української мови і культури, формування російськими засобами масової комунікації викривленої інформаційної картини світу. Серед загроз інформаційній безпеці можна зазначити такі чинники, як відсутність цілісної комунікативної політики держави та недостатній рівень медіа-культури суспільства. Зусилля державної влади мають бути направлені на зміцнення єдності українського суспільства. Культурна та освітянська політики мають бути визначені як актуальні складові державної політики національної безпеки.

Необхідно зазначити, що в інформаційній сфері, а саме в теле- і медіапросторі, існує потреба в локалізації проявів агітації та пропаганди колабораціонізму, як це було донедавна на трьох відомих телеканалах, на яких дозволялася недопустима фривольність, направлена на підрив національної безпеки. Однак державна влада, як і відповідні спецслужби, проявляли певну терпимість до явних антиукраїнських інформаційних передач. А тому існує потреба в прийнятті законопроекту про кримінальну відповідальність та протидію колабораціонізму та сепаратизму, і в напрацюванні відповідних державних програм про системну протидію пропаганді ворога. Зазначене надасть державі правовий інструмент для заборони колабораціоністських структуру, включаючи і політичні партії. Однак, для цього потрібні прояв політичної волі і, що надто актуально, належної професійної реакції

спецслужб і правоохоронних органів України на зазначені загрози. Тим самим будуть усунуті спекулятивні твердження про утискання «свободи слова» в України.

Література

1. Перша і друга Гаазькі конвенції та Декларації 1899 і 1907 рр. URL : https://uk.wikipedia.org/wiki/%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B5_%D0%B3%D1%83%D0%BC%D0%B0%D0%BD%D1%96%D1%82%D0%B0%D1%80%D0%BD%D0%B5_%D0%BF%D1%80%D0%B0%D0%B2%D0%BE (дата звернення : 05.02.2021).

2. Гаазькі конвенції 1907 р. URL : https://zakon.rada.gov.ua/laws/main?find=2&dat=19070000&user=a&text=&textl=1&bool=and&org=0&typ=20&datl=0&yer=1907&mon=00&day=00&numl=2&num=&minjustl=2&minjust= (дата звернення : 05.02.2021).

3. Женевські конвенції 1949 р. URL : https://zakon.rada.gov.ua/laws/main?find=2&dat=19490000&user=a&text=&textl=1&bool=and&org=0&typ=20&datl=0&yer=1949&mon=00&day=00&numl=2&num=&minjustl=2&minjust= (дата звернення : 05.02.2021).

УДК 355.40

Куцій М.С.
Національна академія Служби безпеки України

ВРАЗЛИВІСТЬ СИСТЕМИ ЯК ПРОБЛЕМА РЕАЛІЗАЦІЇ ВІДКРИТОЇ АРХІТЕКТУРИ НА ОБ'ЄКТАХ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

У лютому 2021 року в Microsoft визнали правоту незалежного дослідника "Йонаса Л." (@jonasLyk) [1] щодо існування небезпечної вразливості у версіях Windows, починаючи з XP і до збірок W 10 build 1803 та Update 2018 року. Її суть полягає в тому, що від однорядкової команди пошкоджується файлова система NTFS жорсткого диску. Команду можна виконати не маючи облікового запису Windows із привілеями. Для спрацювання помилки (англ. – bug) достатньо спровокувати доступ до атрибуту *NTFS $i30*, але в особливий спосіб, заклавши "баг" у файл ярлика, ZIP-архів, batch-файли тощо. Команда миттєво пошкоджує файлову систему та щоб виправити проблему комп'ютер пропонує перезавантаження, після якого головна файлова таблиця (MFT) диску вже містить пошкоджений запис. Отже, з невідомих на сьогодні причин у системі через цей "баг" не спрацьовує розділ реєстру, який повинен відповідати за т. з. синій екран смерті (BSoD).

На офіційній веб-сторінці [2] урядової команди реагування на інциденти безпеки CERT-UA, що функціонує в рамках Держспецзв'язку України, інформація про означену вразливість відсутня. З метою спростування чи

підтвердження існування цієї помилки в конкретній операційній системі Windows замість робочого технічного засобу безпечніше скористатися віртуальною машиною із дзеркальною Windows, яку краще привести у дію в операційній Linux на іншому комп'ютері.

На сьогодні в державних установах на категорованих та некатегорованих об'єктах електронно-обчислювальної техніки застосовуються усі версії Microsoft Windows, у т.ч. вищевказані різновиди її збірок.

Отже, з 2001 року – року створення багатокористувацької операційної Windows XP та до сьогодні лише через вразливість NTFS $i30 у всіх системах Windows існує небезпека цілісності інформації, вимога щодо захисту якої встановлена чинним законодавством. При цьому, в автоматизованих системах класу "1" окремих підприємств, військових частин та організацій продовжується застосування операційних Windows 7 і Windows XP, програмну підтримку яких Microsoft припинено з січня 2020 року та квітня 2014 року відповідно. Вищенаведене не викликає сумнівів, що Microsoft здійснить усунення вразливості NTFS $i30 починаючи лише з багатокористувацької версії Windows 8.1.

Відповідно до ДСТУ 3396.2-97 [3] до означеної помилки ставимося як до передумови штучного (спеціально створеного) порушення цілісності та блокування інформації технічними каналами.

Принцип *відкритої архітектури* інформаційної системи є принципом інформаційної безпеки та полягає в тому, що ця безпека не може забезпечуватись через якусь *неясність*. Спроби захистити інформаційну систему шляхом приховування її слабких місць лише відстрочує за часом вірусну або інсайдерську атаку.

Отже, такою неясністю протягом останніх 20 років залишаються причини пошкодження запису MFT при застосуванні в системах Windows "бага" NTFS $i30.

Висновки. Використання на державних об'єктах ЕОТ комерційних програмних засобів іноземного походження із закритим вихідним кодом не завжди сприяє реалізації принципу відкритої архітектури при побудові комплексів технічного захисту інформації. Автор розглядає як пріоритетну для безпеки держави розробку для її установ лише вітчизняних базових програм, що виконують керування апаратною складовою та обчислювальним процесом автоматизованих систем. З огляду на досвід деяких розвинутих країн, це, передусім, можуть бути створені в Україні на державне замовлення системи на базі ядра Linux.

Література

1. Jonas L. NTFS Vulnerability criticality underestimated. [Електронний ресурс]. – Режим доступу: https://twitter.com/jonasLyk/ status/1347900440000811010?ref_ (дата звернення 09.02.2021).

2. Офіційна веб-сторінка CERT-UA. [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/about-us (дата звернення 09.02.2021).

3. Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97. Офіційний сайт Держспецзв'язку України. [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ (дата звернення 09.02.2021).

УДК 004.912

Ланде Д.В.
доктор технічних наук, професор
Дмитренко О.О.
Інститут проблем реєстрації інформації НАН України

ПОБУДОВА ОНТОЛОГІЧНИХ МОДЕЛЕЙ У ГАЛУЗІ ПРАВА

Внаслідок швидкого розвитку інформаційно-телекомунікаційних технологій відбувається стрімке накопичення даних у вигляді найрізноманітніших джерел – файлів, електронних листів, вебсторінок та інших джерел не залежно від форматів їх подання. Науково-технічний прогрес вплинув, зокрема, й на правову галузь. Кількість нормативно-правових документів поданих у електронному вигляді, а отже, і кількість інформації, з якою доводиться мати справу експерту у цій сфері, теж постійно зростає. Тож актуальною для правової галузі є задача спрощення доступу до головного змісту тексту, виокремлення з нього головних викладок, ідей та заздалегідь заявлених змістових аспектів. Також не менш важливим є завдання виявлення дублюючої інформації та протиріч у нормативно-правових документах. Це призводить до необхідності розвивати та удосконалювати наявні технологічні рішення та розробляти нові з метою забезпечити достатньо високу швидкість обробки й аналізу правової інформації.

Під час вибору методів дослідження та побудови термінологічних онтологій в галузі права потрібно враховувати той факт, що на відміну від величезних об'ємів неструктурованих даних, які знаходяться у вільному доступі на інформаційних ресурсах у вебмережі, правова інформація у певній мірі є структурованою, але водночас не завжди доступна для вільного перегляду.

Оскільки задача комп'ютеризованої обробки текстів лежить на перетині лінгвістичних і математичних наук, то для побудови онтологічної моделі, придатної для автоматизованої обробки, у цій роботі пропонується застосовувати лінгвомережеву модель представлення текстових даних. У такій мережі вершинами є ключові слова та словосполучення, а зв'язками – семантико-семантичні зв'язки, які присутні у реченні між цими ключовими

термінами. Для виокремлення ключових термінів застосовується розмічування частин мови за допомогою наявних програмних засобів комп'ютерної обробки природномовних текстів. Враховуючи те, до якої частини мови належить кожне слово у тексті, здійснюється формування термінів та їх подальше статистичне зважування [1]. Крім того з розміченого тексту пропонується вилучити стоп-слова, які не несуть собою ніякого інформаційного навантаження.

Для побудови ненаправлених зв'язків у мережі термінів застосовувався алгоритм горизонтальної видимості [2], а для встановлення напрямків зв'язків враховувалась інформація про те, до якої частини мови належить кожен термін [3]. Апробація запропонованого підходу була здійснена на основі вільнодоступних правових документів, поданих англійською мовою.

Загалом, запропонована методика побудови термінологічних онтологій може бути використана у системах автоматичного реферування правової інформації. Це сприятиме формуванню й удосконаленню понятійного і термінологічного апарату у правовій галузі та гармонізації національного і міжнародного права.

Література

1. Lande D.V., Radziievska O.H.: Subject Domain Models of Jurisprudence According to Google Scholar Scientometrics Data // Proceedings of the 4th International Conference on Computational Linguistics and Intelligent Systems (COLINS 2020). Volume I: Main Conference. Lviv, Ukraine, April 23-24, 2020. CEUR Workshop Proceedings (ceur-ws.org). - Vol-2604. - pp 32-43. ISSN 1613-0073. [http://ceur-ws.org/Vol-2604/paper3.pdf].

2. Lande, D. V., Snarskii, A. A., Yagunova, E. V., & Pronoza, E. V.: The use of horizontal visibility graphs to identify the words that define the informational structure of a text. In: 2013 12th Mexican International Conference on Artificial Intelligence, pp. 209-215 (2013).

3. Ланде Д.В., Дмитренко О.О. Методика виокремлення ключових слів і словосполучень та побудови направлених зважених мереж термінів із застосуванням Part-of-Speech tagging. Інформаційні технології і безпека // Матеріали XX Міжнародної науково-практичної конференції ІТБ-2020. - Київ: Інжиніринг. - С. 140-144. ISBN: 978-966-2344-77-6.

УДК 004.056
Лаптєв О.А.
доктор технічних наук,
старший науковий співробітник
Гребенніков А.Б.
Лаптєв С.О.
Загиней А.Ю.
Державний університет телекомунікацій

МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ НЕЛІНІЙНИХ ПАРАМЕТРАХ ЗОВНІШНІХ ВПЛИВІВ З УРАХУВАННЯМ ВЗАЄМОДІЇ КОРИСТУВАЧІВ

Інформація яка цікава для будь-якого користувача в основному залежить від характеристик останнього. Більш того, користувачі зі схожими характеристиками схильні спілкуватися один з одним. Уявімо епідемічну модель з ймовірністю передачі певної інформації, як функції відстані між джерелом і потенційною метою. Далі буде показано, що ця епідемічна модель не має кордонів мережі має обмежувальний поріг, що має на увазі – поширення інформації обмежено.

З урахуванням нелінійного характеру зовнішніх впливів, для розробки моделі захисту інформації з урахуванням взаємовпливу користувачів, будемо використовувати рівняння:

$$\begin{cases} \dfrac{dI}{dt} = \alpha Z + \beta_1 I - \sum\limits_{k=2}^{\infty} L_k I_0^k \sin^k \omega t, \\ \dfrac{dZ}{dt} = \beta_2 I + \gamma - \sum\limits_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} \quad (1)$$

де $\alpha = Z_p$, $\beta_1 = C_v + C_K$, $\beta_2 = -\left(C_{d2} + C_{d1}\right)$, $\gamma = (\alpha + \beta + \theta + \rho)V$ (2)

Вирішуючи систему рівнянь 1 відносно коефіцієнту захисту, отримуємо модель системи захисту інформації в соціальної мережи в залежності від коефіцієнта взаємодії користувачів.

Остаточне рівняння розробленої моделі у загальному вигляді буде мати вигляд:

$$Z(t)=\int[-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)-\beta_1((\alpha+\beta+\theta+\rho)V)+\beta_1\sum_{k=2}^{\infty}K_kZ_0^k\sin^k\omega t]\times$$

$$[\left(-C_{d2}-C_{d1}\right)\times\sum_{k=2}^{\infty}L_kI_0^k\sin^k\omega t]\times$$

$$\times\left((1-e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\frac{e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}})-(1-e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\frac{e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}}\right)dt \qquad (3)$$

Де: V_i – коефіцієнт, що відображає вплив загроз інформації від взаємодії між користувачами на захищеність інформаційної системи;

α – описує схильність суб'єкта до встановлення взаємодії;

β – описує привабливість або популярність;

θ – описує шлях інформації;

ρ – характеристика тенденцій моделі до симетричності діад.

З метою підтвердження отриманих теоретичних результатів, проведемо моделювання за розробленою моделлю захисту інформації при нелінійних параметрах зовнішніх впливів з урахуванням взаємодії користувачів.

Рис. 1. Графік захисту інформації з урахуванням взаємодії користувачів та інтенсивності передачі інформації

Аналіз графіка рис. 1 показує, що зі зростанням коефіцієнтів взаємодії користувачів та інтенсивності передачі інформації захист інформації зростає. Зростання коефіцієнтів взаємодії користувачів та інтенсивності передачі інформації приводять до зростання захисту інформації в соціальної мережі, що відповідає дійсності та доводить вірогідність отриманих результатів.

Особливістю за пропанового методу є те, що крім загальної оцінки кількості інформації у системи. Ми використовуємо коефіцієнт, що відображає вплив загроз інформації від взаємодії між користувачами на захищеність

інформаційної системи З зростанням кількості інформації та взаємодії користувачів зростає параметр захисту інформації в соціальної мережі, що відповідає фізичному сенсу.

Додаткова особливість запропонованого методу полягає у тому, що ми використовуємо параметри: схильність суб'єкта до встановлення взаємодії та привабливість або популярність інформації. Але ця особливість базується на прийнятих обмеженнях. Більш детальні параметри захисту інформації персональних даних ми не враховуємо, що може у де яких випадках привести до похибки визначення захищеності даних.

Висновки. Таким чином, розроблена модель захисту інформації при нелінійних параметрах зовнішніх впливів з урахуванням взаємодії користувачів у результаті моделювання. За допомогою розробленої моделі, отримали параметрі захисту інформації, якій дозволяє проводити аналіз системи захисту після зовнішніх впливів на систему захисту. Модель дозволяє проводити дослідження параметрів захисту системи та вживати необхідні заходи для поліпшення системи захисту інформації з урахуванням нелінійних параметрів зовнішніх впливів та специфіки соціальної мережи.

Література

1. Yevseiev S., Laptiev O., Lazarenko S., Korchenko A., Manzhul I. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31

УДК 321.1

Мацик Ю.Й.
Міністерство цифрової трансформації України

РОЗВИТОК ІНТЕРНЕТУ ТА КІБЕРГІГІЄНА

У сучасному світі є беззаперечним фактом, що збільшення рівня доступності та швидкості Інтернету сприяють економічному зростанню країни. Прискорення розгортання широкосмугового зв'язку має важливе значення не лише з точки зору його потенціалу для зростання ВВП, але й для забезпечення сучасним зв'язком бізнесу та громадян.

До 2020 року були відсутні дані щодо наявності фіксованого ШСД у розрізі кожного населеного пункту України. У 2019-2020 роках Мінцифри було проведено детальне всеукраїнське дослідження щодо покриття волоконно-оптичними технологіями у всіх населених пунктах України.

Станом на травень 2020 року якісний фіксований ШСД доступний для 85% населення України. Показник проникнення фіксованого ШСД серед домогосподарств в Україні становить 46%, тоді як середній показник в ЄС становить 78% , а у найбільш розвинених країнах 82% .

Що стосується мобільного зв’язку, на сьогодні є розрахункові дані, надані операторами щодо наявності мереж LTE. Станом на вересень 2019 року 4G був доступний у 8 230 містах, в яких проживає 73% населення. Відсоток абонентів, які користуються мобільним ШСД на початок 2020 року становив 64% . При цьому, відсоток термінального обладнання, яке підтримує відповідні покоління зв’язку, становить 69%, тобто майже усі абоненти, у яких є відповідне обладнання, користуються послугами ШСД.

Програмою діяльності Кабінету Міністрів України передбачено до 2024 року забезпечити 95% жителів України можливістю користуватися мобільним і фіксованим швидкісним інтернетом. Тобто, громадяни зможуть отримати послугу доступу до Інтернету майже в усіх населених пунктах України.

У поточному році Законом України «Про державний бюджет України на 2021 рік» передбачено видатки на закупівлю послуг фіксованого Інтернет-доступу для 6000 соціальних закладів (навчальні заклади, заклади медицини, культури), що розміщені у 3000 сіл, в яких швидкісний Інтернет недоступний. Територіальні громади зможуть отримати субвенцію з державного бюджету для замовлення послуг з підключення соціальних закладів зі швидкістю 100 Мбіт/с, близько 1.5 млн мешканців сільської місцевості вперше отримають можливість підключитись до швидкісного Інтернету.

Цифровий світ – це обмін приватною інформацією, де одна сторона розкриває свої ідентифікаційні дані та реквізити платіжних інструментів, а інша їх обробляє, перевіряє, підтверджує, зберігає та відповідно надає послуги. Причому той, хто розкриває інформацію, має бути впевненим, що його приватні дані належно зберігаються та неправомірно не використовуються.

На сьогоднішній день в умовах сучасної цифровізації суспільства актуальними стають питання:

- безпеки дітей;
- контенту доступного дітям;
- збереження приватної інформації;
- правил безпеки у цифровому середовищі.

Провідні ВУЗи України у партнерстві з Проектом CRDF Global розпочали співпрацю з міжнародними експертами з кібербезпеки та на своїй базі проводять онлайн-курси "Базові правила безпеки у цифровому середовищі".

«Кібергігієна» - це розвинуті навички користувачів цифрового середовища, що спрямовані на захист персональних даних та чутливої приватної інформації.

Оскільки шкода від втрати або несанкціонованого власником розкриття приватної інформації може завдати значних втрат як фізичній особі

так і бізнесу, то існує потреба розвитку навичок кібергігієни на рівні загальноосвітніх шкіл і післяшкільної освіти. Здібність класифікувати за чутливістю приватну інформацію, розпізнавати зловмисні програми та розуміти способи їх дії стають невід'ємною складовою цифрових навичок.

На сьогодні у державі існує проблема цифрової освіти. Шкільний курс «Основи інформатики» має адаптуватись під розвиток сучасних цифрових навичок та основ кібергігієни. У закладах післяшкільної освіти мають з'явитись обов'язкові предмети з кібербезпеки та кібергігієни.

УДК 351.86

Мельник Д.С.
кандидат юридичних наук,
Національна академія Служби безпеки України

ЩОДО СУЧАСНИХ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Згідно зі ст. 1 Закону України «Про національну безпеку України» загрози національній безпеці це «явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів і збереження національних цінностей України».

Актуальні загрози національній безпеці України в інформаційній сфері свого часу були визначені Стратегією національної безпеки України (Розділ 3), затвердженою Указом Президента України від 26.05.2015 № 287/2015 (втратила чинність), а також у чинній Концепції розвитку сектору безпеки і оборони України (Розділ II) та доповнені й уточнені в Стратегії кібербезпеки України (Розділ 2): комп'ютерна злочинність та комп'ютерний тероризм; розвідувально-підривна діяльність іноземних спецслужб організацій, груп, осіб у кіберпросторі; широка присутність в інформаційній інфраструктурі України пов'язаних з РФ суб'єктів; політично вмотивовані кібератаки на урядові та приватні веб-сайти; уразливість автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури до кібератак; реалізація іноземними державами, міжнародними злочинними угрупованнями кіберзагроз щодо автоматизованих систем державного та військового управління, об'єктів критичної інформаційної інфраструктури; застосування новітніх технологій як для скоєння традиційних, так і принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації; використання інформаційних ресурсів об'єктів критичної інфраструктури для фінансування тероризму, сепаратизму та розповсюдження зброї масового знищення тощо.

Окрім того, у п. 4 Доктрини інформаційної безпеки України, затвердженій Указом Президента України від 25.02.2017 № 47/2017, визначені наступні загрози, які досі зберігають свою актуальність в сучасних умовах:

– здійснення спеціальних інформаційних операцій (СІО) проти України;

– проведення РФ СІО в інших державах з метою створення негативного іміджу України у світі;

– інформаційна експансія РФ та контрольованих нею структур, у т.ч. шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

– інформаційне домінування РФ на тимчасово окупованих територіях;

– недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів;

– неефективність державної інформаційної політики, недосконаліть інформаційного законодавства, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;

– поширення закликів до вчинення радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Вказані загрози інформаційній безпеці України переважно узгоджуються та якісно доповнюють перелік загроз національній безпеці в інформаційній сфері, сформований у новій Стратегії національної безпеки України, затвердженій Указом Президента України від 14.09.2020 № 392/2020 [1].

Зокрема, нова Стратегія національної безпеки України в якості сучасних загроз національній безпеці України в інформаційній сфері визначила:

– стрімкі технологічні зміни та зростання ролі інформаційних технологій у всіх сферах суспільного життя (п. 9);

– застосування Росією інформаційної «зброї» у поєднанні з енергетичною для зміцнення позицій у Європі, її намагання впливати на внутрішньополітичну ситуацію у європейських державах, підживлення триваючих конфліктів, збільшення військової присутності у Східній Європі (п. 16);

– продовження РФ гібридної війни проти України шляхом системного застосування інформаційно-психологічних, кібернетичних, політичних, економічних і воєнних засобів для відновлення свого впливу на неї (п. 17);

– внутрішню і зовнішню деструктивну пропаганду, що розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність, використовуючи суспільні протиріччя в умовах відсутності цілісної інформаційної політики держави, слабкості системи стратегічних комунікацій (п. 20);

– недостатню ефективність державних органів, що ускладнює вироблення і реалізацію державою ефективної політики (у т.ч. в інформаційній

сфері), є джерелом загроз незалежності України, її суверенітету і демократії (п. 22);

– посилення загроз для критичної інфраструктури (у т.ч. її інформаційної складової), пов'язаних з погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, зокрема фізичним і кібернетичним, триваючими бойовими діями, а також тимчасовою окупацією частини території України (п. 27).

З урахуванням приписів п. 66 нової Стратегії національної безпеки України має бути підготовлена Стратегія інформаційної безпеки України, потребує оновлення чинна Стратегія кібербезпеки України. Наприкінці лютого цього року робоча група при Національному координаційному центрі кібербезпеки РНБО України схвалила проєкт Стратегії кібербезпеки України на 2021–2025 роки [2].

Автори проекту Стратегії кібербезпеки України констатують зростання питомої ваги кіберзагроз у спектрі загроз національній безпеці країн, а також критично зростаючий технічний рівень інструментарію реалізації цих загроз.

Поряд із низкою вже відомих і досі актуальних кіберзагроз – зростаючою кіберзлочинністю та кібертероризмом в національному сегменті кіберпростору: розвідувально-підривною діяльністю у кіберпросторі спецслужб іноземних держав, насамперед РФ, проти України, активним використання РФ кіберпростору у гібридній війні проти України та для фінансування терористичних угруповань, недостатнім рівнем захисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури від кібератак тощо, розробники проекту визначають як загрозу невпинне нарощення арсеналу кіберзброї наступального, розвідувального та підривного призначення, а також поширення використання кіберпростору для вчинення не лише кібернетичних, але й інших видів злочинів (проти основ національної безпеки, легалізації доходів, одержаних злочинним шляхом, торгівлі людьми, незаконного обігу зброї, наркотиків та інших небезпечних предметів і речовин) тощо.

При цьому виділяються низка небезпечних чинників, які по суті не є загрозами, однак носять характер ризиків для національної безпеки у кіберпросторі: невідповідність вимогам законодавства стану захисту ІТС державних органів та суб'єктів господарювання; недооцінка загроз, що виникають у кіберзахисті державних інформаційних ресурсів; незабезпечення кіберзахисту електронних інформаційних ресурсів значної частини підприємств, установ та організацій усіх форм власності; висока технологічна залежність України від іноземних виробників продукції ІКТ та програмного забезпечення; відсутність сучасних національних стандартів вимог з безпеки розроблення програмного забезпечення та ІТС, систем сертифікації

або оцінки відповідності з безпеки такої продукції, а також ланцюга поставок відповідного обладнання; витоки інформації з баз даних популярних соціальних мереж, веб-сайтів, реєстрів тощо, які збирають велику кількість ідентифікаційних та персональних даних користувачів; низький рівень кіберграмотності населення; недостатній рівень взаємодії України з міжнародними партнерами у протидії кібертероризму та кіберзлочинності тощо.

В сучасних умовах рівень забезпечення *інформаційної безпеки України безпосередньо залежить від якісної* організації системи протидії загрозам національній безпеці в інформаційній сфері та ефективного захисту національних інтересів. Основні напрями діяльності держави для забезпечення її національних інтересів і безпеки у т.ч. в інформаційній сфері наразі визначені у розділі ІІІ нової Стратегії національної безпеки України. У свою чергу пріоритетні напрямами державної політики щодо забезпечення інформаційної безпеки закріплені у п. 5 Доктрини інформаційної безпеки України та розділі 4 Стратегії кібербезпеки.

Саме за цими напрямами мають формуватися конкретні шляхи та інструменти захисту національних інтересів і безпеки України в інформаційній сфері, які визначатиме майбутня Стратегія інформаційної безпеки як головний документ щодо організації діяльності уповноважених суб'єктів у цій сфері відповідно до п. 66 нової Стратегії національної безпеки України.

Література

1. Указ Президента України від 14.09.2020 № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.

2. Робоча група при НКЦК РНБО України схвалила проєкт Стратегії кібербезпеки України. URL: https://www.rnbo.gov.ua/ua/Diialnist/4838.html.

УДК 004.94.355

Міхєєв Ю. І.
кандидат технічних наук,
Житомирський військовий інститут імені С. П. Корольова

ШЛЯХИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ В НАЦІОНАЛЬНОМУ СЕГМЕНТІ КІБЕРПРОСТОРУ

Результати аналізу тенденцій реформ у політиці держави, а саме внутрішньої інформаційної політики з питань протидії загрозам в кіберпросторі дозволив виокремити завдання з покращення інформаційно-аналітичного забезпечення відповідних структур. Тому сьогодні актуальним постає питання удосконалення системи інформаційно-аналітичного забезпечення

Збройних Сил України у сфері кібербезпеки з урахуванням набутого досвіду під час виконання завдань відповідними підрозділами у Антитерористичній операцій та операції Об'єднаних сил та підходів країн-членів НАТО.

Специфіка інформаційно-аналітичного забезпечення пов'язана з обробкою великих обсягів даних, а саме: сортування, класифікація, доповнення, порівняння, аналіз інформації у формах, зручних для розуміння кінцевому користувачу; систематизація зібраних матеріалів шляхом виділення фактичних даних, що стають підґрунтям для певних висновків [1]. Виконання вище зазначених завдань стає неможливим без використання спеціалізованого програмного забезпечення інформаційно-аналітичного спрямування. У провідних країнах світу активно застосовуються такі програмні продукти, зокрема аналітичні платформи: IBM I2, Maltego, Splunk та інші [2].

Тому одним з можливих шляхів удосконаленні системи інформаційно-аналітичного забезпечення Збройних Сил України у сфері кібербезпеки є розроблення вітчизняного спеціалізованого програмного забезпечення визначеної спрямованості із застосуванням найсучасніших підходів оброблення великих обсягів даних, інтелектуального аналізу тексту, імітаційного моделювання, нейронних мереж та інших, а також активне його впровадження на практиці в повсякденну діяльність відповідних підрозділів.

В умовах удосконалення системи інформаційно-аналітичного забезпечення Збройних Сил України виникає завдання з раціонального удосконалення системи інформаційно-аналітичного забезпечення органів державної влади у сфері кібербезпеки. Це потребує вирішення завдання з визначення спроможностей інформаційно-аналітичного забезпечення підрозділів Збройних Сил України та розгляду ряду питань з:

аналізу основних завдань інформаційно-аналітичного забезпечення підрозділів Збройних Сил України та умов їх виконання для ефективного реагування на загрози національній безпеці у воєнній сфері;

обґрунтування вимог до спроможностей інформаційно-аналітичного забезпечення підрозділів Збройних Сил України з урахуванням стану захищеності кібербезпеки держави;

розроблення методичного апарату оцінювання цих спроможностей, для подальшого аналізу місць у системі, що можуть бути удосконалені та виключення вразливих місць у функціонуванні системи інформаційно-аналітичного забезпечення;

розроблення варіантів побудови системи інформаційно-аналітичного забезпечення Збройних Сил України спираючись на потреби підрозділів в системі кібербезпеки держави.

Підходи до розроблення системи інформаційно-аналітичного забезпечення Збройних Сил України мають враховувати стандарти НАТО та інформаційно-аналітичне забезпечення в національному сегменті кіберпростору.

Отже, основні напрямки удосконалення інформаційно-аналітичного забезпечення Збройних Сил України полягають в застосуванні сучасних інформаційних технологій, що дозволять автоматизувати деякі завдання відповідних підрозділів та розроблення системи інформаційно-аналітичного забезпечення з урахуванням оцінки їх спроможностей.

Література

1. Варенко В. М. Інформаційно-аналітична діяльність: Навч. посіб. / В. М. Варенко. – К.: Університет "Україна", 2014. – 417 с.

2. Гнусов Ю.В. Використання інформаційно-аналітичних інструментів у сфері боротьби з кіберзлочинністю / Ю.В. Гнусов, Ю.М. Онищенко // Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукраїнського науково-практичного семінару (25 листопада 2016 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2016. – С. 22-24.

УДК 355.40

Огарок А.П.
кандидат технічних наук, професор,
Військова частина А1906

ПІДХІД ДО СТВОРЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ РОЗВІДУВАЛЬНИХ ОРГАНІВ УКРАЇНИ

Останнім часом у спецслужбах іноземних держав приділяється велика увага модернізації та вдосконаленню систем і комплексів технічної розвідки, нарощуванню їх можливостей щодо несанкціонованого доступу до об'єктів критичної інфраструктури інших країн, проведенню спеціальних інформаційних операцій. З огляду на ці обставини, особливої ваги набувають питання вдосконалення систем забезпечення інформаційної безпеки (далі – СЗІБ) силових органів державної влади України [1], передусім розвідувальних органів, які оперують значним обсягом цінної конфіденційної інформації, створення необхідних умов їхнього функціонування в нових реаліях геополітичної обстановки. Вирішити це завдання можливо шляхом створення максимально надійної системи забезпечення інформаційної безпеки, побудованої на сучасних організаційних і технологічних розробках, результатах спеціальних наукових досліджень, враховуючи специфічні вимоги до захисту інформації, зумовлені конкретними потребами сфери розвідувальної діяльності.

У доповіді висвітлено характерні вимоги до такої системи, підходи до об'єднання окремих заходів і засобів захисту в загальну інтегровану систему, з погляду на сучасні загрози інформаційній безпеці [2–3]. Головним

завданням створення такої системи є досягнення максимальної ефективності захисту інформаційного ресурсу розвідувального органу на основі комплексного застосування необхідних методів і засобів, що виключають несанкціонований доступ до конфіденційної і таємної інформації. Наголошується, що для створення такої системи, необхідно знайти оптимальне рішення завжди присутньої в такій ситуації суперечності: з одного боку, – забезпечити максимально надійний захист інформації, тобто виключити як випадковий, так і навмисний доступ до інформаційних ресурсів сторонніх осіб, розмежувати доступ до пристроїв системи всіх користувачів; з другого, – система не повинна створювати помітні незручності користувачам під час їхньої роботи з ресурсами. Досягнути реальний рівень захисту інформації розвідувального органу можна шляхом об'єднання в цілісну систему організаційних і технологічних прийомів, розробивши комплекс спеціальних засобів і методів захисту інформації.

У виступі наголошено на будові системи організаційно-технологічного (соціотехнічного) типу, де загальну організацію захисту та виконання поставлених завдань забезпечує керівництво і співробітники розвідувального органу (організаційна складова), а безпосередній захист інформації здійснюється паралельно з технологічними процесами її обробки (технологічна складова). Підхід до будови такої системи має ураховувати особливості об'єкта впроваджуваної системи, оцінку ймовірних загроз безпеці об'єкта, аналіз способів та засобів, якими необхідно оперувати, створюючи систему, оцінку економічної доцільності її створення, співвідношення внутрішніх і зовнішніх загроз та можливість внесення необхідних змін у процесі функціонування системи. Ключовим пунктом у розробленні СЗІБ є визначення ймовірних джерел виникнення загроз безпеці інформації розвідувального органу. При цьому джерела загроз слід розглядати як сукупність явищ, факторів та умов, що реально створюють небезпеку витоку конфіденційної інформації. Тому, зважаючи на особливості службових і управлінських процесів розвідувального органу, необхідно окреслити множину загроз, критичних для цього органу, з метою вироблення уточнених заходів захисту та протидії.

Впроваджувати заходи зі створення СЗІБ доцільно на трьох напрямах: адміністративному, організаційному і програмно-технічному. Адміністративний напрям передбачає формулювання керівництвом розвідувального органу мети та програми виконуваних робіт у напрямі створення (модернізації) системи забезпечення безпеки інформаційного ресурсу, планування необхідного фінансового та матеріального забезпечення, контролю виконання запланованих заходів. Організаційний напрям включає вирішення питань створення умов ефективного функціонування служби, відповідальної за режим захисту інформаційного ресурсу, проведення комплексу про-

філактичних заходів. Технічний напрям передбачає розгляд програмно-технічних засобів, що реалізують задані вимоги. Якщо вимоги сформульовані в термінах функцій (сервісів) безпеки, розглядаються механізми безпеки й відповідні їм варіанти програмних та апаратних реалізацій. Якщо вимоги сформульовані по підсистемах інформаційної системи, розглядаються варіанти програмно-апаратної реалізації цих підсистем.

Запропонований підхід до формування СЗІБ розвідувального органу передбачає, передусім, вжиття заходів своєчасного виявлення та запобігання можливих ризиків, а не усунення їх наслідків. Використання принципу об'єднання окремих заходів і засобів захисту в загальну інтегровану схему запобіжних заходів у процесі моделювання системи забезпечення конфіденційності, цілісності та доступності інформації є найбільш раціональним підходом до створення оптимізованої за вартістю та функціоналом системи інформаційної безпеки розвідувального органу.

Література

1. Доктрина інформаційної безпеки України: Указ Президента України від 25 лютого 2017 року N 47/2017. URL: https://www.president.gov.ua/documents/472017-21374.

2. Левченко О.В. Інформаційні загрози як різновид воєнних загроз державі /О.В. Левченко, Ю.І. Михеєв // Наука і техніка Повітряних Сил Збройних Сил України. ЖВІ С.П. Корольова, Житомир – 2018. – № 3(32). – С. 14–19.

3. Косогов О.М. Інформаційна безпека у сфері оборони як складова воєнної безпеки України / О.М. Косогов // Системи обробки інформації. – 2016. № 8 (145), м. Харків. – С.115–117. URL: https:/www.hups.mil.gov.ua

УДК 343.3/.7

Олєйніков Д.О.
кандидат юридичних наук,
Інститут підготовки юридичних кадрів для СБУ
Національного юридичного університету ім. Я. Мудрого

ЩОДО НЕОБХІДНОСТІ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Обираючи об'єкти кримінально кримінально-правової охорони і встановлюючи кримінально-правові заборони, законодавець повинен враховувати, перш за все, соціальну обумовленість правового припису, цінність окремих суспільних відносин, їх роль та значення для всієї системи суспільних відносин [1, с. 171]. Ефективність норми кримінального права визначається, з одного боку, її соціальною обумовленістю, з іншого ж боку, необ-

хідно враховувати правильність конструювання складу злочину, яка є важливою умовою практичної реалізації принципів кримінального права, зокрема – принципу законності.

В.В. Кузнецов визначає кримінально-правову охорону як певну систему кримінально-правових засобів, до яких слід включити кримінально-правові норми (заборонні, роз'яснювальні, заохочувальні та обмежувальні) та методи кримінально-правової політики (криміналізація та декриміналізація, пеналізація та депеналізація), за допомогою яких нормативність права переводиться в упорядкованість суспільних відносин [2, с. 109].

Інформаційна безпека, з одного боку, передбачає забезпечення якісного всебічного інформування громадян та вільного доступу до різних джерел інформації, а з іншого – це контроль за непоширенням дезінформації, сприяння цілісності суспільства, збереження інформаційного суверенітету, протидія негативним інформаційно-психологічним пропагандистським впливам та захист національного інформаційного простору від маніпуляцій, інформаційних війн та операцій. Рішення комплексної проблеми інформаційної безпеки дасть змогу як захистити інтереси суспільства і держави, так і гарантувати права громадян на отримання всебічної, об'єктивної та якісної інформації [3, с. 27].

В Доктрині інформаційної безпеки України, затвердженій Указом Президента України від 25 лютого 2017 року № 47/2017 наголошується, що застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України. При цьому зазначається, 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 [4].

З цього приводу О.П. Єрменчук підкреслює, що «…Україна протистоїть найсерйознішому за роки своєї незалежності виклику у сфері забезпечення державної безпеки. Військовий конфлікт на сході країни, торгівельні війни, економічна експансія, різке посилення тероризму, небувалий ріст злочинності, руйнування та пошкодження численних підприємств, у тому числі стратегічно важливих, інфраструктурних об'єктів, втрата новітніх технологій – все це та інші ризики вимагають від держави нових підходів до завчасного виявлення загроз та їх попередження і припинення» [5, с. 5].

Погодимось із М.Т. Гаврильцівим у тому, що система інформаційної безпеки держави є складовою частиною загальної системи національної

безпеки країни та становить сукупність органів державної влади, недержавних структур і громадян, які повинні узгоджено здійснювати діяльність по забезпеченню інформаційної безпеки на основі єдиних правових норм, ефективно протистояти інформаційним загрозам за сучасних умов [6, с. 203]. Чим обумовлені особливості вітчизняної кримінально-правової охорони інформаційної безпеки? По-перше, існуючі норми розраховані, перш за все, на протидію внутрішнім загрозам, та є мало орієнтованими на сучасну динаміку та еволюцію злочинної діяльності як у кіберпросторі, так і в реальному середовищі. По-друге, вітчизняним законодавцем так і не сформовано ефективний кримінально-правовий інститут, який би поєднував багаторівневий захист інтересів держави в інформаційній безпеці як від внутрішніх, так і від зовнішніх загроз.

Інформаційна безпека як окремий об'єкт злочину не розглядається наукою кримінального права, тому її кримінально-правова охорона здійснюється через відповідні кримінально-правові норми, які розміщені законодавцем в різних розділах Особливої частини КК України. Не вдаючись до обґрунтування, віднесемо до таких складів злочину ті, що передбачені ст.ст. 111, 114, 328, 329, 330, 333 та Розділом XVI Особливої частини КК України. Разом з цим, якщо піддати іншу частину статей детальному науковому аналізу, то частина норм також передбачає кримінальну відповідальність за дії, які очевидно посягають на інформаційну безпеку держави.

Враховуючи цю обставину, в першу чергу необхідно переглянути перелік загальних об'єктів кримінально-правової охорони, передбачений ст. 1 КК України, та визначити за вертикаллю роль і місце інформаційної безпеки держави на рівні, наприклад, видового об'єкту, а окремих її складових – безпосереднього. На підставі отриманих висновків доцільно сформувати відповідний інститут злочинів проти інформаційної безпеки держави, доповнивши його новими нормами, які передбачають кримінальну відповідальність за посягання на інформаційну безпеку держави (наприклад, посягання на інформаційну інфраструктуру об'єктів критичної інфраструктури).

Література

1. Коржанский Н.И. Объект и предмет уголовно-правовой охраны / Н.И. Коржанский. – М.: Юридическая литература, 1980. – 248 с.

2. Кузнецов В. В. Кримінально-правова охорона: проблеми визначення поняття / В. В. Кузнецов // Науковий вісник Ужгородського національного університету. Серія : Право. - 2015. - Вип. 30(2). - С. 107-110.

3. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам / У. Ільницька // // Humanitarian vision. – 2016. – Vol. 2, Num. 1. – С. 27-32.

4. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47/2017. Режим доступу : https://www.president.gov.ua/documents/472017-21374.

5. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монограф. / О. П. Єрменчук. Дніпро : Дніпроп. держ. ун-т внутр. справ, - 2018. - 180 с.

6. Гаврильців М.Т. Інформаційна безпека держави у системі національної безпеки України / Гаврильців М.Т. // Юридичний науковий електронний журнал. - 2020. - № 2. - С. 200-203.

УДК 343.98

Онищенко Ю.М.
кандидат наук з державного управління, доцент
Світличний В.А.
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ

ПІДХОДИ ДО УДОСКОНАЛЕННЯ ДЕРЖАВНИХ МЕХАНІЗМІВ БОРОТЬБИ З КІБЕРЗЛОЧИННОСТЮ

Сьогодні економічна, соціальна та військова безпека будь-якої держави значною мірою залежить від гарантування безпеки в інформаційній сфері. Державна політика захисту інформації та кібернетичної безпеки, її повнота та ефективність забезпечують стабільність у суспільстві, дотримання прав і свобод громадян. В основному Законі України у ст. 17 відзначається, що забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього Українського народу [1].

Паралельно зі стрімким розвитком інформаційних технологій (далі – ІТ) та активним їхнім використанням у всіх сферах життя сучасного соціуму, збільшується кількість використання ІТ та глобальної мережі Інтернет з протиправними намірами.

Незважаючи на зовні різну природу двох найпомітніших останніми роками соціальних феноменів – глобалізації злочинності та появи глобального інформаційного мегасередовища, виявляється дуже жорсткий їх зв’язок і тенденція до його зміцнення. Взаємозалежність цих суспільних проявів виходить далеко за межі електронно-кримінального явища, що визначається терміном «комп’ютерна злочинність» або «кіберзлочинність».

Глобалізація інформаційних процесів і поява глобального інформаційного простору, який за своєю суттю є нематеріальним і поки що в повному обсязі не є законодавчо врегульованим (сама можливість подібного врегулювання – дуже суперечливе питання), призводить не лише до появи нових об’єктів злочинних посягань – комп’ютерів і комп’ютерних мереж. З’являються нові способи скоєння злочинів, наприклад здійснення розкрадань шляхом зміни або блокування комп’ютерних даних. Інші наслідки повсюд-

ного поширення ІТ – майже безперешкодне формування і пропаганда кримінальної ідеології, використання інформаційного простору в кримінальних цілях – для зв'язку і обміну досвідом, координації дій тощо.

Кіберзлочинність є однією з найактуальніших проблем сучасності, оскільки негативно впливає на діяльність органів державної влади та органів місцевого самоврядування, а завдана нею шкода стосується різних сфер суспільної життєдіяльності, зменшує рівень довіри до державного апарату в цілому. Ефективність запобігання і протидії кіберзлочинності засобами державного управління безпосередньо залежить від узгодженості дій та заходів усіх суб'єктів, наявна система яких, їх функціональна та організаційно-штатна структура є недосконалими. З урахуванням цього можна стверджувати, що серед актуальних проблем сучасного державного управління чільне місце належить дослідженню механізмів запобігання і протидії кіберзлочинності.

Проблематику забезпечення державного управління у сфері запобігання і протидії кіберзлочинності в Україні в умовах світової глобалізації не систематизовано, щобільше, подекуди не визначено й найбільш суттєвих загроз. А це, у свою чергу, призводить до нехтування досвідом передових країн світу, які вже мають напрацювання та формалізовані методики боротьби з кібератаками, кіберінцидентами, кіберзлочинами, нарешті – кібертероризмом.

До основних напрямів подальшого розвитку державних механізмів боротьби з кіберзлочинністю в Україні можна віднести удосконалення: правового механізму забезпечення взаємодії між органами державної влади в частині впорядкування нормативно-правових актів за схемою: концепція → стратегія → пакет нормативно-правових актів; інституціонального механізму – шляхом проведення відповідних організаційно-штатних змін для оптимізації структури державних органів, що опікуються забезпеченням кібербезпеки.

Дослідження проблем боротьби з кіберзлочинністю показало, що орієнтація тільки на технічні та технологічні засоби забезпечення інформаційної безпеки (технічний захист інформації) в умовах інформатизації, у тому числі профілактики кіберзлочинів, не має значного успіху [2].

Чим складніше стає комп'ютерне програмно-математичне забезпечення, тим більше уразливими виявляються традиційні організаційні заходи і засоби інженерно-технічного захисту інформації в автоматизованих (комп'ютерних) системах, зокрема відносно несанкціонованого доступу.

Проблемою наступного порядку також є і те, що з розвитком сучасних електронних засобів інформації розвиваються й технічні засоби перехоплення і доступу до інформації, яка обробляється і передається в електронних системах зв'язку. Доступ до цих засобів не створює проблеми для злочинних формувань.

Найбільшу небезпеку для суспільства і держави складає трансгранична організована кіберзлочинність: комп'ютерний тероризм; диверсії, інші прояви антагоністичної інформаційної боротьби кримінальних формувань з державою, правоохоронними органами; крадіжки інформації з комп'ютеризованих баз даних і порушення права інтелектуальної власності на комп'ютерні програми; шахрайства з використанням комп'ютерних технологій, особливо у сфері міжнародних економічних відносин (кредитно-фінансова, банківська) тощо.

Трансграничний характер кіберзагроз змушує країни вступати в тісну міжнародну співпрацю, яка потрібна не лише для ефективної підготовки до захисту від кібератак, але і для своєчасної реакції на них, ліквідації наслідків.

Література

1. Конституція України // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – с. 141. – URL:https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення 09.03.2021).

2. Орлов О.В. Організаційні та нормативно-правові засади боротьби з кіберзлочинністю / О.В. Орлов, Ю.М. Онищенко // Державне управління: удосконалення та розвиток. – 2014. – № 5. – URL:http://www.dy.nayka.com.ua/?op=1&z=715 (дата звернення 09.03.2021).

УДК 355.40:358.12

Оніщук В.С.
Національний університету оборони України
імені Івана Черняховського

ОСОБЛИВОСТІ ВВЕДЕННЯ ПСИХОЛОГІЧНОГО ВПЛИВУ

Коли розповсюдження інформації про негативну громадську думку впливає на політичні концепції людей, це часто призводить до того, що в першу чергу люди мають різні думки про правлячу групу. Неорганізовані та неузгоджені політичні відносини між людиною та правлячою групою неминуче призводять до конфліктів. Основні засоби масової інформації почали критикувати або ставити під сумнів неоконсервативну глобальну стратегію та політику. Є багато книжкових видань, таких як "Занепад влади Сполучених Штатів", "Кінець американської ери", "Смуток імперії: кінець мілітаризму, таємність і республіканізм", "Пузир верховенства США", "Вибір: глобальне домінування або глобальне лідерство", "Надмірність імперії: чому Захід втратить війну з тероризмом" та інші бестселери. AssociatedPress також повідомила, що 20-річне покоління молодих людей навколо Сполучених Штатів Америки розглядає військове зловживання ув'язненими на телебаченні і "Записали, як вони сумні, ганебні та розчаровані". Все це сильно стимулювало протистояння між громадськістю США

та адміністрацією Буша. Січень-лютий 2004 року випуск "AtlanticMonthly" сказав: "Гострими цілями американців є Пентагон, Республіканська партія, Буш і багатонаціональні корпорації". Білл Шнайдер, який утримує CNN, сказав: "Сполучені Штати ніколи не поділялися подібним чином з часів Другої світової війни".

Поширення інформації про негативну думку також впливає на міжособистісні та соціальні відносини. Коли громадська думка ізраїльського населення повідомляла про цілеспрямовану домовленість органів влади з палестинським рухом "Хамас", вона навмисно стверджувала, що це було наслідком таємничих домовленостей (які були конфіденційними). Мета полягала в тому, щоб зробити кожного в палестинському суспільстві самокритичним, без взаємної турботи, співпраці та підтримки, лише зі взаємною підозрою та ворожнечею. Фактично, "праведна поведінка", "страти брата та батька за вбивство сина" прийшли один за одним в Палестині. Хоча це і ліквідувало деяких зрадників, але й спричинило крайню напруженість міжнаціональних відносин, та не сприяло розвитку боротьби [1].

Виділяються три типи пропаганди – біла, сіра та чорна. Біла пропаганда – це пропаганда, що поширюється та визнається джерелом інформації або його офіційними представниками. Сіра – це пропаганда, яка спеціально не ідентифікує своє джерело інформації. Чорна – це та, яка презентується, видається вихідною із іншого джерела замість достовірного. Окрім цього пропаганда може бути позитивною та негативною. Негативна (деструктивна) пропаганда нав’язує людям ті або інші переконання за принципом “мета виправдовує засоби”. Мета негативної пропаганди – розпалювання соціальної ворожнечі, нагнітання соціальних конфліктів, загострення суперечностей у суспільстві, пробудження низинних інстинктів у людей тощо. Це роз’єднує людей, робить їх слухняними волі пропагандиста. Основна функція негативної пропаганди – створення ілюзорної, паралельної реальності з “перевернутою”, або спотвореною системою цінностей, переконань, поглядів. Негативна пропаганда активно використовує низьку критичність та навіюваність мас, щоб маніпулювати цими масами в інтересах невеликої групи осіб [2].

Заради війни ворог повинен запустити кампанії з використанням засобів масової інформації для запуску атак, плутанини чи приховування його планів або взагалі не мають нічого спільного та зловживають. Це вимагає того, щоб під час пошуку ворожих пропагандистських відомостей воно мало бути обширним та систематичним. Необхідно не тільки звернути увагу на отримання інформації про основні новинні ЗМІ, але також обережно ставитесь до ворогів, використовуючи деякі, що, здавалося б, "не беруть участі у війні" і "не занепокоєні війною". Промислові та групові інформаційні ЗМІ та ЗМІ, які їдуть нейтрально країни та групи. У сучасній високотехнологічній війні ми повинні бути особливо пильними проти інфор-

маційних атак, запущених ворогом, використовуючи Інтернет. Коротше кажучи, всі пропагандистські повідомлення від ворога повинні бути зібрані та освоєні якомога більше, а інформація з усіх засобів масової інформації повинна бути надана жорсткій увазі та обережності.

Перевірка надійності та достовірності інформації, отриманої в результаті проведення збори в відкритих джерелах. Результати проведення збори в відкритих джерелах істотно залежать від надійності і достовірності цих джерел. При цьому розрізняються основні та додаткові джерела [3].

Таким чином, після того як ми правильно виявили правильний змову ворога, ми повинні використовувати публічну дипломатію для організації потужної контратаки. У контратаці перша полягає в тому, щоб відкрито виставити пропагандистський план противника. У той же час ми повинні знайти можливості виявити слабкі місця пропаганди ворога та розпочати "антипропаганду" ворогу. Розкриваючи ворожі пропагандистські змови, ми також повинні повністю враховувати доцільність термінів та тактичної гнучкості. Вибір того, який вид термінів і які методи та тактику використовувати для розкриття пропагандистського плану супротивника, повинні повністю ґрунтуватися на реальних потребах національної політики та тактики дипломатичної боротьби та операцій.

Література

1. Вооруженные силы зарубежных государств: информационно-аналитический сборник / А.Н. Сидорин, Г.М. Мингатин, В.М. Прищепов, В.П. Акуленко. – М.: Воениздат, 2009. – 528 с.

2. Социальные сети: модели информационного влияния, управления и противоборства / Д.А. Губанов, ДА. Новиков, А.Г. Чхартишвили. – М.: ФИЗМАЛИТ, 2010. – 228с.

3. Основи стратегії національної безпеки та оборони держави: підруч. / О.П. Дузь-Крятченко, Т.М. Дзюба, А.О. Рось, ін. – 2-ге вид., доп. і випр. – К.: НУОУ, 2010. – 591 с.

УДК 351/354:621.395.97:004.738.5.057.4

Осьмак А.С.
PhD з публічного управління та адміністрування,
Національна академія державного управління
при Президентові України

ЦИФРОВІ ГОЛОСОВІ КОМУНІКАЦІЇ В ПУБЛІЧНОМУ УПРАВЛІННІ. КЛАСИФІКАЦІЯ ТА БЕЗПЕКА

Соціальні обмеження, викликані пандемією COVID-19, значно змінили глобальний комунікаційний ландшафт та спричинили активний розвиток інструментів цифрових комунікацій: конференцій, у тому числі відеоконференцій, месенджерів, чат-ботів тощо. Значна частина комунікацій, у тому

числі й управлінських, перейшла в онлайн форму. Активне використання систем відеоконференцій показало, що візуальна інформація є подекуди надлишковою, оскільки основне смислове навантаження несе саме мовна (вербальна, словесна) комунікація. Серед голосових сервісів, паралельно з класичною телефонією, все частіше використовуються голосові цифрові інтернет комунікації.

Термін комунікація, походить від латинського communicatio (повідомлення, передача), що є похідним від communis (спільний) [1] – процес обміну інформацією між двома або більше особами із метою передавання та одержання інформації. Також варто зазначити, що комунікативна підсистема публічного управління охоплює суб'єктів взаємодії, інформаційні зв'язки й управлінські відносини, процеси взаємодії суб'єктів управління між собою та з іншими суспільними інститутами. [2].

Поштовхом до нового етапу розвитку цифрових голосових комунікацій став запущений у 2020 році розробником програмного забезпечення Alpha Exploration Co сервіс Clubhouse (Клабхаус) – соціальна мережа, що ґрунтується виключно на голосовому спілкуванні. Під впливом росту популярності сервісу Clubhouse – голосові мережі для групових трансляцій в режимі реального часу анонсували основні світові лідери IT-індустрії, такі як:

– Telegram, який запустив функцію створення чатів виключно для групового голосового спілкування та трансляцій без можливості відправки текстових повідомлень [3];

– Facebook анонсував розробку соціальної мережі, в якій всі користувачі спілкуються виключно голосом [4];

– Twitter анонсував запуск голосових сервісів Spaces для користувачів на базі Android та iOS [5];

– Stereo App Ltd., представив сервіс, який дозволяє здійснювати голосові комунікації/трансляції в режимі реального часу [6];

Усі голосові інтернет комунікації об'єднує технологія VoIP (voice over IP – голос через IP) – передача медіа даних у режимі реального часу за допомогою сімейства протоколів TCP/IP, у якій аналоговий звуковий сигнал абонента дискретизується, компресується й пересилається цифровими каналами зв'язку до іншого абонента (групи абонентів), де проводиться зворотна функція – декомпресія, декодування й відтворення аналогового сигналу. Проте, поява нових можливостей голосових інтернет комунікацій для вимагає більш чіткої класифікації таких сервісів за функціональним призначенням. Так нині можна виділити 4 функціональні типи цифрових голосових інтернет сервісів:

– передача коротких голосових повідомлень (voice message, voicemail);

– IP-телефонія;

– групові немодеровані голосові сервіси / конференції;

– групові модеровані / трансляційні голосові сервіси.

Маючи на ринку інформаційних послуг велику кількість програмних продуктів для цифрових голосових комунікацій та передбачаючи перспективу попиту на такі сервіси серед користувачів, перед органами публічної влади виникає питання вибору номенклатури сервісів, чіткого визначення сфер застосування, формування корпоративних вимог, як до переліку сервісів так і до правил їх використання та безпека передачі даних. Для цього насамперед варто визначити сферу використання таких продуктів – це внутрішні та зовнішні комунікації. Для зовнішніх комунікацій голосові сервіси можуть використовуватись як додаткові канали в процесі масових публічних комунікацій та консультацій.

Для внутрішніх комунікацій органів публічної влади цифрові голосові сервіси можуть застосовуватись у процесі внутрішніх комунікацій, вироблені управлінських рішень, ситуаційній координації, проведенні голосових нарад тощо. Внутрішня (корпоративна) комунікативна політика, у тому числі в сфері публічного управління, має визначити номенклатуру систем для забезпечення процесу внутрішньої комунікації, враховувати інтероперабельність та вимоги до конфіденційності та криптозахисту.

Література

1. Етимологічний словник української мови: у 7 т. / [гол. ред. О. С. Мельничук]. – К.: Наук. думка, 1985. – Т. 2.

2. Дрешпак В. М. Комунікації в публічному управлінні : навч. посіб. / В. М. Дрешпак. – К. : ДРІДУ НАДУ, 2015. – 168 с. http://biblio.umsf.dp.ua/jspui/bitstream/123456789/3136/1/Комуніації в публічному управлінні.pdf.

3. Voice Chats Done Right https://telegram.org/blog/voice-chats?ln=r.

4. Mike Isaac. Facebook Is Said to Be Building a Product to Compete With Clubhouse. *The New York Times. Feb. 10, 2021* https://www.nytimes.com/2021/02/10/technology/facebook-building-product-clubhouse.html.

5. Kim Lyons. Twitter users on Android can now join the platform's Clubhouse-like Spaces. *The Verge. Mar 2, 2021.* https://www.theverge.com/ 2021/3/2/22309629/twitter-launches-spaces-android-ios-audio-clubhouse.

6. Vivian Iroanya. What is the Stereo app? Everything you need to know about the newest rival to Clubhouse. *The Tab. Jan 29, 2021.* https://thetab.com/uk/2021/01/29/what-is-the-stereo-app-everything-you-need-to-know-about-the-newest-rival-to-clubhouse-192918.

УДК 004.056.5

Павленко М.М.
Бондарчук А.А.
Житомирський військовий інститут імені С.П. Корольова

ШЛЯХИ СТВОРЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ

Розвиток та впровадження інформаційних технологій в усі сфери життєдіяльності суспільства потребує постійного забезпечення кібернетичної

безпеки як невід'ємної складової національної безпеки держави. Особливо актуальним є забезпечення кібернетичної безпеки в умовах ведення гібридних війн у сучасних збройних конфліктах. Для підвищення обороноздатності та забезпечення національних інтересів у кіберпросторі збройні сили (ЗС) розвинених держав світу проводять комплекс організаційних та технічних заходів, спрямованих на оперативне адекватне реагування на виклики та загрози, пов'язані з появою новітніх розробок у сфері інформаційних технологій (ІТ) та інтенсивним розвитком апаратних та програмних засобів кібернетичної зброї.

Питання всебічного аналізу сучасного стану системи кібернетичної безпеки держави та надання пропозицій щодо удосконалення потенціалу сектора безпеки та оборони України в сфері кібербезпеки має актуальний характер.

Гібридна війна, яка відбувається між Росією і Україною, включає не тільки воєнні дії та інформаційно-психологічні операції, а й кібернетичні атаки. Підтверджено факти використання шкідливого та вірусного програмного забезпечення (контенту) Turla/Uroburos/Snake, RedOctober, MiniDuke, та NetTraveler.

За досвідом останніх років можна виділити основні об'єкти кібернетичних атак на наступне десятиліття:

атомні електростанції;

об'єкти критичної інфраструктури в енергетичній, соціальній та банківській сферах;

камери систем міського відеонагляду;

інформаційно-телекомунікаційні системи органів влади;

інші об'єкти критичної інфраструктури.

Головні проблеми забезпечення кібернетичної безпеки України постають з таких причин:

відсутності чіткого усвідомлення ролі та значення кібербезпеки як складової в системі забезпечення інформаційної безпеки держави;

дефініційної, термінологічної та нормативно-правової неврегульованості у сфері кібернетичної безпеки;

масове використання державними організаціями програмних і технічних продуктів іноземного виробництва та піратського програмного забезпечення;

відсутності належної координації діяльності відповідних відомств, неузгодженості дій зі створення окремих елементів системи кібернетичної безпеки;

дефіциту щодо методичного забезпечення та кадрового наповнення відповідних структурних підрозділів.

Згідно з положеннями Стратегії кібербезпеки України, удосконалення потенціалу сектора безпеки та оборони України в сфері кібербезпеки має

здійснюватися за рахунок реалізації різних заходів, основними серед яких мають бути такі:

1) Захист на об'єктах критичної інфраструктури технологічних процесів від несанкціонованого втручання в їх роботу, на яких контроль або моніторинг відбувається за допомогою інформаційно-комунікаційних систем.

2) Державне стратегічне планування та управління в сфері електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту шляхом впровадження інформаційно-комунікаційних систем.

3) Створення центру кіберуправління у ЗС України для забезпечення кібербезпеки і кіберзахисту на стратегічному, оперативному і тактичному рівнях, у яких всі процеси управління мають відбуватися за допомогою інформаційно-комунікаційних систем.

4) Створення підрозділів кібербезпеки і кіберзахисту у ЗС України, СБ України, Національній поліції України та інших силових структурах, досягнення їхньої сумісності з відповідними підрозділами держав-членів НАТО, у яких контроль та моніторинг за всіма процесам має відбуватися за допомогою інформаційно-комунікаційних систем.

5) Розроблення та впровадження протоколів спільних дій з названими підрозділами у відповідних силових структурах, зокрема, й обмін інформацією в режимі реального часу, організація швидкого реагування на кіберзагрози та кібератаки за допомогою інформаційно-комунікаційних систем.

Таким чином, можна зробити наступні висновки: Україна продовжує створення повноцінної системи національної кібернетичної безпеки. Основним механізмом обрано реалізацію Стратегії забезпечення кібернетичної безпеки України. Це відбувається на фоні активної агресії РФ у кіберпросторі, що має на меті отримання непублічних відомостей та проведення кібератак на сайти органів державної влади. На сьогодні та наступне десятиліття реальні прояви кібератак на інформаційні ресурси України можуть призвести до порушень функціонування інформаційно-телекомунікаційних систем як звичайної, так і критичної інфраструктури, які безпосередньо впливають на стан національної безпеки й оборони держави. У зв'язку із цим наявні та потенційно можливі гібридні загрози вимагають впровадження державою комплексних заходів щодо забезпечення її кібернетичної безпеки.

Література

1. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа; за заг. ред. д-ра техн. наук, професора В.Б. Толубка.— Київ: ДУТ, 2015. – 288 с.

2. Грицюк Ю.І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання / Науковий вісник НЛТУ України: збірник науково-технічних праць. – Львів : РВВ НЛТУ України. – 2016. – Вип. 26.8. С.327-337.

УДК 340.1
Пилипчук В.Г.
доктор юридичних наук, професор, академік НАПрН України,
НДІ інформатики і права НАПрН України

ПРОБЛЕМИ ТА ПРІОРИТЕТИ РОЗВИТКУ ПРАВОВОЇ НАУКИ В КОНТЕКСТІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ, ЗАХИСТУ ПРАВ ТА БЕЗПЕКИ ЛЮДИНИ, СУСПІЛЬСТВА І ДЕРЖАВИ

В сучасних умовах глобалізації інформаційного простору, цифрової трансформації та розбудови інформаційного суспільства, стрімкого впровадження інформаційно-комунікаційних технологій, штучного інтелекту та інших інформаційних (цифрових) технологій, продуктів і послуг формуються новітні суспільні відносини у різних сферах життєдіяльності людини, суспільства, держави та міжнародної спільноти, а також нові виклики і загрози у сфері інформаційної, кібернетичної, національної та міжнародної безпеки.

Водночас, у провідних країнах світу відбуваються процеси підготовки та впровадження так званого *шостого технологічного устрою*[*], який за оцінками низки вітчизняних та іноземних експертів буде включати складові двох рівнів:

Перший рівень – *новітні технології промислового виробництва, нова інфраструктура та системи управління (на глобальному, регіональному (субрегіональному) і національному рівнях);*

Другий – *цифрова економіка.*

Відповідно, за наявними прогнозними оцінками, країни світу за цих умов можуть поділитися на три групи:

– країни, які будуть володіти складовими обох рівнів шостого технологічного устрою, у тому числі системою управління;

– країни, що будуть мати лише цифрову економіку;

– країни, які не будуть мати жодної складової вказаного технологічного устрою.

За цих умов відповідно постане й питання щодо визначення цифрового майбутнього України та її місця в сучасному глобалізованому світі.

[*] За оцінками експертів і вчених, *п'ятий технологічний устрій* характерний для постіндустріального суспільства, *четвертий* – для індустріального суспільства, *третій технологічний устрій* – для аграрного суспільства.

За нашими оцінками[1], а також висновками низки іноземних експертів і вчених, застосування новітніх технологій промислового виробництва та цифрової економіки сприятиме не лише створенню нових продуктів і послуг та розширенню можливостей людини, а також може призвести до низки негативних соціально-економічних наслідків, зокрема, *зростання безробіття, соціального розшарування населення, посилення кризових процесів* тощо.

Крім цього, як свідчать результати досліджень, в умовах запровадження штучного інтелекту буде стрімко актуалізуватися проблема співвідношення між реальним (людським) і штучним інтелектом, а також створеними внаслідок їх взаємодії цифровими алгоритмами. В контексті зазначеного варто звернути увагу, що останніми роками експерти і вчені констатують процеси спрощення навчального процесу та певне наближення його до машинних алгоритмів. Як наслідок, відбувається формування, передусім у дітей і молоді, т.зв. «цифрової свідомості» та психологічної залежності від інформаційно-комунікаційних технологій. У багатьох випадках ця залежність створює прямі загрози їх життю і здоров'ю.

З цього приводу також слід зауважити, що штучний інтелект та відповідні алгоритми у багатьох країнах, у т.ч. в Україні, вже використовуються на практиці для ідентифікації осіб, фіксації правопорушень, а також несанкціонованого збору і обробки персональних даних та інших характеристик приватного життя людини. Про вказане, зокрема, свідчать рішення судів США, Іспанії та інших держав щодо притягнення до юридичної відповідальності низки транснаціональних корпорацій *(Google, Facebook та ін.)* за вказані протиправні дії.

---

[1] *Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін.* Захист прав, приватності та безпеки людини в інформаційну епоху: монографія / Пилипчук В.Г., Брижко В.М., Доронін І.М., Золотар О.О., Батиргареєва В.С., Богуцький П.П., Радзієвська О.О., Тарасюк А.В., Ткачук Т.Ю.; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ – Одеса : Фенікс, 2020. 260 с.; *В. Куйбіда, В. Бебик, М. Дмитренко, В. Пилипчук та ін.* Національна безпека в умовах інформаційних та гібридних війн : монографія / авт. кол.: В. Куйбіда, В. Бебик, М. Дмитренко, В. Пилипчук та ін.; за заг. ред.. В. Куйбіди і В. Бобика. – Київ : НАДУ, 2019. – 384 с.; *Пилипчук В.Г., Компанцева Л.Ф., Кудінов С.С., Доронін І.М. та ін.* Становлення і розвиток системи стратегічних комунікацій сектору безпеки і оборони України : монографія / В.Г. Пилипчук, Л.Ф. Компанцева, С.С. Кудінов, І.М. Доронін, О.В. Акульшин, О.П. Дзьобань, О.Г. Заруба; за заг ред. Пилипчука В.Г. – К.: ТОВ «Видавничий дім «АртЕк», 2018. – 274 с.; *Пилипчук В.Г., Брижко В.М., Баранов О.А., Мельник К.С.* 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 ред. В.М. Брижка, В.Г. Пилипчука. – К.: ТОВ "Видавничий дім "АртЕк", 2017. – 226 с. та ін.

Водночас, новітні інформаційні (цифрові) технології активно використовуються для ведення сучасної гібридної війни, проведення інформаційних та психологічних операцій, здійснення кібератак на об'єкти критичної інфраструктури, скоєння терористичних актів та інших злочинів і правопорушень.

Загалом, сучасні трансформаційні процеси потребують кардинального перегляду державної політики, системи управління, забезпечення безпеки тощо. Актуальність цього наочно підтверджують останні події, пов'язані із запровадженням карантинно-обмежувальних заходів у зв'язку з поширенням короновірусної хвороби COVID-19 та розширенням застосування інформаційних технологій у сфері законотворчої діяльності, державного управління, у фінансово-економічній, медичній, освітній та інших сферах.

Відповідні системні заходи у цій сфері нині здійснюються на рівні Апарату РНБО України, Комітету Верховної Ради України з питань цифрової трансформації і Міністерства цифрової трансформації, а також МВС України, СБ України, Державної служби спеціального зв'язку і технічного захисту інформації України та інших державних органів.

Зазначене, як свідчить аналіз, потребує комплексного наукового опрацювання у різних галузях науки, зокрема, в галузі права.

З цією метою Науково-дослідним інститутом інформатики і права НАПрН України за участі представників Секції права національної безпеки та військового права НАПрН України було запропоновано при підготовці *Стратегії розвитку Національної академії правових наук України на 2021 – 2025 роки* передбачити такі пріоритетні напрями фундаментальних і прикладних наукових досліджень в галузі права:

– правове забезпечення інформаційної сфери;

– правове забезпечення у сфері цифрової трансформації;

– правове забезпечення у сфері національної безпеки та оборони.

При цьому, щодо ***правового забезпечення у сфері цифрової трансформації*** вперше запропоновано виокремити такі пріоритетні напрями досліджень:

1) філософські й теоретико-правові основи формування і розвитку суспільних відносин в умовах цифрової трансформації; теорія, методологія і напрями правового забезпечення цифрової трансформації у різних сферах життєдіяльності людини, суспільства, держави та міжнародної спільноти;

2) правові засади формування і реалізації державної політики у сфері цифрової трансформації, розвитку системи державного управління у цій сфері; правове регулювання створення та виробництва складових систем та засобів цифрової трансформації, розвитку цифрової інформаційної інфраструктури, ринку електронних комунікацій, користування радіочастотним ресурсом;

3) теоретико-методологічні засади формування і розвитку новітніх правових засад щодо визначення понять, критеріїв, змісту та обсягів правоздатності, дієздатності й деліктоздатності штучного інтелекту і робототехніки, опрацювання проблем визначення їх спеціальної або загальної правосуб'єктності та юридичної відповідальності у цій сфері;

4) правовий режим проектування, виробництва, впровадження та експлуатації сучасних систем і засобів цифрової трансформації та їх основних складових (технологій Інтернету речей, штучного інтелекту, робототехніки, криптовалют, технологій блокчейн, «хмарних» технологій, «великих даних», електронних комунікацій та соціальних мереж);

5) правове забезпечення функціонування опорних кластерів розвитку для проведення цифрової трансформації у промисловості (Індустрія 4.0), в банківський сфері, енергетиці, освіті, державному управлінні, ретейлі, у сільському господарстві, «розумному» містобудуванні, у системі охорони здоров'я, науці та освіті тощо;

6) проблеми правового регулювання з питань застосування автономних (безпілотних) транспортних засобів на основі використання технологій штучного інтелекту (автомобілів, літальних апаратів, морських та річних суден та ін.) з урахуванням прогнозованих змін міжнародного права про відкрите море, дорожній рух, цивільну авіацію тощо;

7) теоретико-правові основи захисту прав та безпеки людини, суспільства і держави в умовах застосування штучного інтелекту, робототехніки, хмарних технологій і технологій блокчейну, соціальних мереж, а також визначення юридичної відповідальності за правопорушення у цій сфері;

8) законодавство зарубіжних країн, порівняльне законодавство у сфері цифрової трансформації; гармонізація та імплементація норм правових актів Європейського Союзу та міжнародного права в законодавство України відповідно до її зобов'язань; правові засади міжнародного співробітництва у сфері цифрового майбутнього.

З питань ***правового забезпечення у сфері національної безпеки та оборони*** до вказаної Стратегії мають бути включені такі пріоритетні напрями досліджень:

1) теоретико-правові основи забезпечення національної, інформаційної та кібернетичної безпеки, захисту суверенітету, конституційного ладу, територіальної цілісності України, прав та безпеки людини і громадянина;

2) правові засади формування та реалізації державної політики з питань національної безпеки і оборони, розвитку системи забезпечення національної безпеки, реформування і розвитку суб'єктів сектору безпеки і оборони та оборонно-промислового комплексу в контексті євроатлантичної інтеграції України;

3) теоретичні основи розвитку права національної безпеки, права міжнародної безпеки та військового права; методологічні та прикладні засади розвитку законодавства з питань національної безпеки і оборони, правового забезпечення організації та діяльності суб'єктів сектору безпеки, функціонування недержавних суб'єктів сектору безпеки як складової системи забезпечення національної безпеки України;

4) правові засади забезпечення національної безпеки у зовнішньо - і внутрішньополітичній сферах, у сфері державної безпеки, у воєнній сфері та сфері безпеки державного кордону; модернізація правової політики України щодо стратегій економічної, енергетичної та екологічної безпеки в умовах глобальних і регіональних трансформацій;

5) проблеми боротьби з тероризмом, кібернетичною та організованою злочинністю і корупцією, протидії злочинам проти основ національної безпеки, проти миру і безпеки людства та міжнародного правопорядку; законодавчого забезпечення оперативно-розшукової, розвідувальної та контррозвідувальної діяльності;

6) актуальні проблеми забезпечення інформаційної безпеки України як однієї з основних функцій держави; правові та організаційні засади забезпечення кібернетичної безпеки, боротьби з кіберзлочинністю, кібершпигунством та кібертероризмом;

7) правове забезпечення захисту персональних даних, інформації з обмеженим доступом, технічного захисту інформації, запобігання і протидії негативним інформаційним впливам та впливам інформаційних технологій на шкоду людині, суспільству, державі та міжнародному правопорядку;

8) правові аспекти становлення і розвитку демократичного контролю над воєнною організацією, державними і недержавними суб'єктами сектору безпеки; організаційно-правові засади цивільно-військового співробітництва, становлення і розвитку системи стратегічних комунікацій сектору безпеки і оборони та євроатлантичної інтеграції України;

9) правові проблеми формування і розвитку систем регіональної (субрегіональної) та міжнародної безпеки, міжнародного співробітництва у цій сфері та гармонізації національного законодавства з нормами міжнародного права, законодавством ЄС і стандартами НАТО в галузі безпеки і оборони.

В цілому, за нашими оцінками, варто пам'ятати, що в сучасних умовах цифрової трансформації жодна держава світу не здатна ефективно забезпечити національну, інформаційну та кібернетичну безпеку власними силами. За цих умов вкрай актуальним постає питання розробки колективних стратегій та об'єднання зусиль країн світу для захисту прав і безпеки людини, суспільства, держави та міжнародної спільноти.

УДК 003.26.09
Полотай О.І.
кандидат технічних наук, доцент
Масюк Н.А.
Львівський державний університет безпеки життєдіяльності

ПРОФІЛІ МОЖЛИВОСТЕЙ ПОРУШНИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СТРУКТУРНИХ ПІДРОЗДІЛІВ БЕЗПЕКОВИХ СТРУКТУР

Порушник – це особа, яка здійснила спробу виконати дії, які призвели до порушення властивостей інформації, що визначені політикою безпеки.

В табл. 1 показані категорії можливих порушників інформаційної безпеки, що притаманні у відділі інформаційних технологій головного управління ДСНС України, незалежно від обласного підпорядкування.

Таблиця 1

Категорії порушників

Позначення	Визначення категорії	Рівень загрози
	Внутрішні у відношенні до відділу інформаційних технологій ГУ ДСНС	
ПВ1	Технічний персонал, який обслуговує будівлі та приміщення (електрики, сантехніки, прибиральники тощо), в яких розташовані компоненти ІТС.	1
ПВ2	Персонал, який обслуговує технічні засоби (інженери, техніки)	2
ПВ3	Відвідувачі	1
ПВ4	Користувачі ІТС	2
ПВ5	Співробітники підрозділів (підприємств) з розробки та супроводження програмного забезпечення	3
ПВ6	Адміністратори	3
	Зовнішні у відношенні до відділу інформаційних технологій ГУ ДСНС	
ПЗ1	Будь-які особи, що знаходяться за межами контрольованої зони	1
ПЗ3	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ4	Хакери	3
ПЗ5	Співробітники закордонних спецслужб або особи, які діють за їх завданням	4

Якщо аналізувати порушників і проводити оцінку їх можливості реалізувати загрозу, то використовуються наступні фактори, які представлені у табл. 2-6.

Таблиця 2

Специфікація моделі порушника за мотивами здійснення порушень (М)

Позначення	Мотив порушення	Рівень загрози
М1	Безвідповідальність	1
М2	Самозатвердження	2
М3	Корисний інтерес	3
М4	Професійний обов’язок	4

Таблиця 3

Специфікація моделі порушника за рівнем кваліфікації та обізнаності (К)

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загрози
К1	Знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи	1
К2	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем	2
К4	Знає структуру, функції та механізми дії засобів захисту, їх недоліки	3
К5	Знає недоліки та вади механізмів захисту, які вбудовано у системне програмне забезпечення та його недокументовані можливості	3
К6	Є розробником програмних та програмно-апаратних засобів захисту або системного програмного забезпечення	4

Таблиця 4

Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту (З)

Позначення	Характеристика можливостей порушника	Рівень загрози
З1	Використовує лише агентурні методи одержання відомостей	1
З2	Використовує пасивні засоби (технічні засоби перейменування без модифікації компонентів системи)	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути приховано пронесені крізь охорону	3
З4	Застосовує методи та засоби дистанційного (з використанням штатних каналів та протоколів зв'язку) впровадження програмних закладок та спеціальних резидентних програм збору, пересилання або блокування даних, дезорганізації систем обробки інформації.	3
З5	Застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передачі даних).	4

Таблиця 5

Специфікація моделі порушника за часом дії (Ч)

Позначення	Характеристика можливостей порушника	Рівень загрози
Ч1	До впровадження ІТС відділу інформаційних технологій ГУ ДСНС України	1
Ч2	Під час бездіяльності компонентів системи (у неробочий час, під час планових перерв у роботі, перерв для обслуговування та ремонту та ін.)	2
Ч3	Під час функціонування ІТС відділу інформаційних технологій ГУ ДСНС України (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС відділу інформаційних технологій ГУ ДСНС України так і під час тимчасової зупинки компонентів системи	4

Таблиця 6

Специфікація моделі порушника за місцем дії (Д)

Позначення	Характеристика місця дії порушника	Рівень загрози
Д1	Без доступу на контрольовану територію	1
Д2	З контрольованої території без доступу у будинки та споруди	1
Д3	Усередині приміщень, але без доступу до технічних засобів ІТС відділу інформаційних технологій ГУ ДСНС України	2
Д4	З робочих місць користувачів ІТС відділу інформаційних технологій ГУ ДСНС України	2
Д5	З доступом у зони даних	3
Д6	З доступом у зону керування засобами забезпечення безпеки ІТС відділу інформаційних технологій ГУ ДСНС України	4

В таблиці 7, сформовані профілі можливостей порушників всіх категорій з урахуванням зазначених вище факторів. У графі “Ефективний рівень загроз” наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Таблиця 7

Профілі можливостей порушників

Позначення	Визначення категорії	Характер дій порушника					Ефективний рівень загроз
		Мотив порушення	Кваліфікація	Можливості	Час дії	Місце дії	
Внутрішні							
КР1	Відвідувачі	М2-М3	К1-К6	З1	Ч3	Д2-Д4	1
КР2	Обслуговуючий персонал	М1-М3	К1-К2	З1	Ч3	Д2-Д5	1
КР3	Технічний персонал	М1-М3	К1-К3	З2	Ч3	Д2-Д4	2
КР4	Користувачі	М1-М3	К1-К2	З1-З2	Ч2-Ч4	Д2-Д4	2

КР5	Співробітники підрозділів супроводження програмного забезпечення	М1-М3	К1-К6	З2	Ч2-Ч4	Д2-Д5	3
КР6	Адміністратори	М1,М2	К1-К6	З2-З3	Ч1-Ч4	Д2-Д6	4
Зовнішні							
КР7	Будь-які особи, що знаходяться за межами контрольованої зони	М2-М3	К1-К3	З1-З3	Ч3	Д1	1
КР8	Представники організацій, що взаємодіють з технічного забезпечення	М2-М3	К1-К4	З1	Ч3	Д1	2
КР9	Хакери	М2-М4	К1-К6	З4	Ч3	Д1	3

Література

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

2. Петров В.А. Інформаційна безпека. Захист інформації від несанкціонованого доступу в автоматизованих системах / Петров В.А., Піскарьов С.А., Шеїн А.В. – М. : Изд-во Ореан, 1998. – 534 с.

УДК 321.7:070.48

Польовий М.А.
доктор політичних наук, професор,
Донецький національний університет імені Василя Стуса

ТЕХНОЛОГІЧНІ ПРОБЛЕМИ АВТОМАТИЧНОГО ВИЯВЛЕННЯ ПРОРОСІЙСЬКОЇ ПРОПАГАНДИ В МЕРЕЖІ FACEBOOK

В силу особливостей політичної ситуації сучасної України ворожа пропаганда є достатньо небезпечною, внаслідок чого виникає проблема її вчасного відстеження. Згідно з результатами моніторингів (наприклад, "Моні-

торинг регіональних ЗМІ, соціальних мереж для оцінки якості та неупередженості висвітлення виборів у місцевих ЗМІ та виявлення дезінформації, прихованих спроб маніпулювання громадською думкою", здійснений на замовлення Комітету виборців України [1]), найбільше Не викликає сумнівів, що найбільше в межах цієї пропаганди в українському сегменті Facebook саме проросійської, хоча теоретично можливі й інформаційні пропагандистські впливи інших країн.

Отже, пабліки та сторінки у Facebook періодично розміщують пропагандистські матеріали, що актуалізує проблему їх пошуку та своєчасного і адекватного реагування на такі матеріали.

Завдання цього повідомлення – обговорення деяких організаційно-технологічних проблем, пов'язаних саме із своєчасним виявленням проросійської пропаганди, що створює умови для своєчасного реагування. Аналіз змісту заходів із реагування на пропагандистські матеріали, а також засобів такого реагування виходить за межі даного повідомлення.

Слід нагадати, що наразі існує багата майже сторічна традиція складення переліків ознак, що свідчать про належність матеріалу до пропаганди. Першу версію запропонував ще Г.Лассвел напередодні другої світової війни. Вона отримала назву "тестів Лассвела" (див. їх перелік, наприклад: [2, с. 122-123]). Серед безсумнівних переваг цих тестів був досить деталізований перелік ознак, яким має відповідати тестований матеріал, щоб бути унаслідженим до пропаганди. У згадуваному моніторингу напередодні місцевих виборів 2020 року використовувалась дещо інша методика виявлення пропаганди, до якої автор цього повідомлення доклав зусиль, з меншою кількістю ознак пропаганди [3]. Як власне тести Лассвела, так і згадувана методика 2020 року досить непогані для використання, вони дозволяють дійсно унаслідженувати матеріали ЗМІ до пропаганди, але вони мають дві основних вади:

1) вони годяться для використання притомними фахівцями з моніторингу – людьми, що мають певний досвід як проведення моніторингів ЗМІ взагалі, так і пошуку пропаганди;

2) вони передбачають знання цими фахівцями соціально-політичного контексту.

Власне висхідні тести Лассвела, вочевидь, передбачали більш широке знання контексту – вони передбачали знання змісту меседжів ворожої преси на теренах суперника. Це знання теоретично дозволяло виявляти, наприклад, паралелізм у повідомленнях аналізованого видання із повідомленнями ворожої преси. Але практика згадуваного моніторингу показала, що й сучасна методика не позбавляє фахівця з моніторингу необхідності знати хоча б місцевий контекст.

Вказані вади ускладнюють використання цих методик виявлення пропаганди в автоматизованому режимі. А це значно удорожчає, якщо не унеможливлює, власне процес вчасного виявлення пропаганди.

Водночас є очевидною необхідність організації саме автоматизованого, програмного, моніторингу, що дозволило б нам отримувати інформацію не лише про факти розміщення пропагандистських меседжів, а й про динаміку їх кількості в масштабі окремого регіону або цілої країни.

Нами розроблено методику, яка налаштована саме на автоматичне виявлення пропагандистських меседжів в мережі Facebook та, водночас, на вирішення проблеми вказаних вище вад існуючих методів [4]. Ця методика покликана обмежити довільність у визначенні належності тексту до пропаганди шляхом використання розгалуженого словника. Питання врахування контексту, яке складно на задовільному рівні вирішити програмними засобами, ми пропонуємо вирішувати за рахунок використання "дворівневого словника". За допомогою "словника першого рівня" ми визначаємо наявність пропагандистських "прекурсорів" в певних пабліках чи сторінках. а вже потім повторним аналізом за допомогою "словника другого рівня" визначаємо пропагандистські меседжі.

Слід зазначити, що головна ідея пристосування аналітичних ознак до автоматичного аналізу постів у Facebook базується саме на забезпечення максимальної "технологізації" процесу виявлення пропаганди, можливо, за рахунок прийнятних похибок у цьому процесі.

Література

1. Моніторинг регіональних медіа під час виборів 2020 (звіт) // Ізбірком. URL: http://cvu.od.ua/ua/library/monitoring-regionalnih-media-pid-chas-viboriv-2020-zvit_1269.

2. Болган В., Пархітько О., Польовий М., Стеблина Н. Ворожі інформаційні операції: нові виміри, нові виклики, нові медіа. Навчально-практичний посібник / За заг. Ред. В.С. Болган. – Одеса, 2021. – 178 с.

3. Моніторинг регіональних ЗМІ, соціальних мереж. Методологія // Ізбірком. URL: http://cvu.od.ua/ua/library/monitoring-regionalnih-zmi-sotsialnih-merej-metodologiya_1231/

4. Польовий М., Котляр К. Результати тижневого моніторингу одеських соцмереж: “кінець епохи демократії” та пропаганда // Ізбірком. URL: https://izbirkom.org.ua/publications/medialiteracy/2021/rezultati-tizhnevogo-monitoringu-odeskih-socmerezh-kinec-epohi-demokratiyi-ta-propaganda/.

УДК: 355.40:351.746.1
Попутніков В.Б.
кандидат юридичних наук,
Національна академія Служби безпеки України

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРОЦЕСІ КОНФІДЕНЦІЙНОГО СПІВРОБІТНИЦТВА

Служба безпеки України як державний орган спеціального призначення з правоохоронними функціями [1; 2] використовує конфіденційне співробітництво при виконанні покладених на неї завдань щодо протидії загрозам державній безпеці. Згідно з положеннями законодавства України [2-5] держава гарантує конфіденційність відносин з особами, які погодились надавати допомогу СБУ (далі – конфіденти), оскільки така гарантія є важливим елементом їх правового захисту. У свою чергу, конфіденти зобов'язані зберігати таємницю, що стала їм відома у ході виконання оперативних завдань [3, 4].

Забезпечення конфіденційності відносин з особами, які надають допомогу СБУ, набуває особливої актуальності в умовах складної оперативної обстановки.

Автором цих тез за результатами проведеного наукового дослідження сформульовано визначення поняття «забезпечення конфіденційності відносин з особами, які надають допомогу СБУ» – реалізація комплексу правових та організаційних заходів, спрямованих на створення умов для гарантованої захищеності відомостей про факт та зміст конфіденційного співробітництва СБУ з особами, які надають (надавали) їй негласну допомогу у виконанні завдань із забезпечення державної безпеки.

Порушена проблематика у контексті подальшого розвитку інформаційно-телекомунікаційних технологій, як в державі в цілому, так і в системі СБУ зокрема, досить тісно пов'язана зі сферою інформаційної безпеки, що у даному випадку стосується конфіденційного співробітництва.

Водночас, У *Стратегії кібербезпеки України*, затвердженої Указом Президента України від 15.03.2016 № 96/2016 [6], реалізація якої покладається серед інших суб'єктів й на СБУ, зазначається, що переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення **нових загроз національній та міжнародній безпеці**, а також констатується зростання кількості та потужності **кібератак**, вмотивованих інтересами окремих держав, груп та осіб. Відтак, поставлено завдання створити національну системи кібербезпеки (як складову системи забезпечення національної безпеки України), що включатиме, зокрема, посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної бо-

ротьби із кіберзагрозами (у т.ч. кібершпигунством, кібертероризмом та кіберзлочинністю), забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом. При цьому, забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі повинно досягатися комплексним застосуванням сукупності правових, організаційних, інформаційних заходів.

Разом із цим, проведений аналіз засвідчує наявність певних правових прогалин та колізій законодавчих та інших правових актів, що регламентують контррозвідувальну та оперативно-розшукову діяльність, охорону державної таємниці [3-5], неврегульованість деяких організаційних питань з урахуванням тенденцій розвитку оперативної обстановки, що зумовлює потребу вдосконалення правових і організаційних засад забезпечення конфіденційності відносин з особами, які надають допомогу СБУ.

З метою покращання стану **інформаційної безпеки конфіденційного співробітництва** вбачається за доцільне розробити та реалізувати на практиці **довгострокову програму**, яка мала б включати:

- удосконалення у ході імплементації положень нової редакції Закону України «Про Службу безпеки України» [7] правового регулювання питань, пов'язаних із забезпеченням конфіденційності відносин з особами, які надають допомогу СБУ (*закріплення на законодавчому рівні принципу «конфіденційності», можливості встановлення конфіденційних відносин з особами без розкриття перед ними належності співробітника до СБУ, покращання охорони державної таємниці у ході конфіденційного співробітництва тощо, а також корегування відповідних підзаконних нормативно-правових актів*);

- підвищення рівня управлінської діяльності керівної ланки оперативних підрозділів (*планування, реалізація заходів, контроль*);

- запровадження нових сучасних та науково обґрунтованих підходів до організації в системі СБУ оперативного процесу в інтересах посилення конспірації (*шляхом відпрацювання чітких правил поведінки оперативних співробітників та осіб, які перебувають в негласному апараті, обмеження доступу до персональних даних конфідентів та неухильного дотримання режиму секретності, підвищення надійності і безпечності зв'язку з джерелами оперативної інформації з використанням телекомунікаційних пристроїв і технологій, удосконалення механізмів координації діяльності різних оперативних підрозділів СБУ при веденні інформаційно-довідкової роботи і т. ін.*);

- суттєве покращання стану інформаційного, кадрового, психологічного та фінансово-матеріального забезпечення оперативної діяльності органів та підрозділів СБУ.

Література

1. Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII.
2. Закон України «Про Службу безпеки України» від 25.03.1992 № 2229-XII (зі змінами).
3. Закон України «Про оперативно-розшукову діяльність» від 18.02.1992 № 2135.
4. Закон України «Про контррозвідувальну діяльність» від 26.12. 2002 № 374-IV.
5. Закон України «Про державну таємницю» від 21.01.1994 № 3855.
6. Указ Президента України від 15.03.2016 № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27.01.2016 «Про Стратегію кібербезпеки України».
7. Проект Закону України «Про Службу безпеки» щодо удосконалення організаційно-правових засад діяльності Служби безпеки України», Реєстр. № 3196 від 10.03.2020.

УДК 004.7:005

Потій О.В.
доктор технічних наук, професор,
Державна служба спеціального зв'язку та захисту інформації України
Дубов Д.В.
доктор політичних наук, старший науковий співробітник,
Національний інститут стратегічних досліджень
Семенченко А.І.
доктор наук державного управління, професор,
Національна академія державного управління
при Президентові України
Фіщук В.В.
ГО «Інститут цифрової трансформації»

ОРГАНІЗАЦІЙНО-ТЕХНІЧНА МОДЕЛЬ КІБЕРЗАХИСТУ УКРАЇНИ

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України", на Держспецзв'язку покладено завдання впровадження організаційно-технічної моделі (далі – ОТМ) кіберзахисту як складової національної системи кібербезпеки.

ОТМ кіберзахисту є складовою національної системи кібербезпеки та відображає основні цінності та принципи, загальну архітектуру, функції та завдання кіберзахисту як цілеспрямованої діяльності суб'єктів з кіберзахисту із застосування сил та засобів кіберзахисту спрямованої на убезпечення кіберпростору України.

Місія ОТМ – через розвиток зрілості (maturity) національної системи кібербезпеки забезпечити її стійкість (resilience) задля безпечного та сталого функціонування українських об'єктів критичної інфраструктури (ОКІ), систем надання електронних послуг, нейтралізації (зменшення наслідків) кібератак.

Метою впровадження ОТМ кіберзахисту є досягнення Україною високого рівня координації та реалізації ініціатив щодо побудови Національної системи кібербезпеки, забезпечення захисту державних і національних інформаційних ресурсів, стабільного функціонування інформаційно-цифрової інфраструктури державних установ, галузей економіки та бізнесу, отримання соціально-економічних зисків від надійного та безпечного функціонування кіберпростору країни.

В доповіді детально викладені головні цілі та архітектура організаційно-технічної моделі кіберзахисту України.

Висновки. Для кожної з складових архітектури ОТМ характерні власні цілі, принципи, пріоритети, завдання, функції, елементи та механізми реалізації, але які мають сприймати та відповідати базовим принципам та в сукупності забезпечують спроможність реалізувати місію ОТМ.

УДК 355.40:358.12

Прима А.М.
доктор філософії,
Національний університет оборони України
імені Івана Черняховського

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХОДІВ ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ВПЛИВУ РОСІЙСЬКІЙ ПРОПОГАНДІ

Дії російсько-терористичних військ у зоні проведення операції об’єднаних сил суттєво підвищують вимоги до розвідки. Важливим напрямком розвідувальної діяльності в інтересах органів військового управління й надалі залишається постійний та цілеспрямований моніторинг відкритих джерел інформації, у тому числі й інформаційних ресурсів мережі інтернет на предмет виявлення в їх контенті ознак інформаційних операцій проти України. Одержувані у результаті такого моніторингу оцінки рівня загроз інформаційній безпеці держави у воєнній сфері суттєво доповнюють загальну оцінку рівня загрози національній безпеці України [1].

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Проти України застосовуються різноманітні інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України.

Боротьба за перевагу у світовому інформаційному просторі провокує різке зростання реальних та потенційних загроз інформаційній безпеці України. Для ефективного формування системи захисту та протидії негативному інформаційному впливу існує необхідність розглядати загрози національній безпеці нашої держави в інформаційній сфері комплексно за всіма сферами. Загрози проявляються у зовнішньополітичній та внутрішньополітичній сферах, у сфері державної безпеки, науково-технологічній, економічній, соціальній та гуманітарній сферах.

Водночас за сучасних умов найбільшу небезпеку становлять загрози у воєнній сфері, і саме проблема інформаційної безпеки воєнній організації держави у контексті жорсткого інформаційного протистояння під час проведення антитерористичної операції викликає найбільшого занепокоєння і потребує найбільшого зосередження органів державної влади та спеціальних служб.

В умовах гібридної агресії Росії проти України державна інформаційна політика передусім зосереджується на реалізації системи заходів щодо протидії руйнівному інформаційному впливу Кремля, насамперед:

запобігання інформаційним загрозам (викликам, впливам) шляхом здійснення превентивних заходів із забезпечення інформаційної безпеки держави;

виявлення інформаційних загроз та деструктивних впливів, яке полягає у систематичному моніторингу, аналізі й прогнозуванні появи реальних або потенційних інформаційних загроз;

запровадження своєчасних заходів з нейтралізації інформаційних загроз, прогнозування ризиків інформаційній безпеці;

ліквідацію наслідків негативних інформаційних впливів [2].

Важливим етапом при реалізації заходів пов’язаних з виявленням деструктивних впливів, є процедура моніторингу та оцінювання загроз інформаційній безпеці України в цілому та у воєнній сфері зокрема. При цьому у воєнній сфері така процедура має свої та властиві лише їй специфічні особливості, які передбачають:

по-перше, виявлення негативного зовнішнього впливу на особовий склад Збройних Сил нашої держави, його аналіз за якісними і кількісними показниками, визначення форм та способів інформаційної боротьби;

по-друге, встановлення та доведення факту наявності в ньому інформаційних загроз державі у воєнній сфері та оцінювання рівня цих загроз.

Однією з причин актуалізації проявів інформаційних загроз державі є швидкі темпи розвитку та впровадження у повсякденне життя інформаційних технологій, що тісно пов’язані з розвитком мережі Інтернет. Завдяки ній користувачі, у тому числі й військовослужбовці ЗС України, задовольняють власні інформаційні потреби, обумовлені не тільки приватною, а й професійною діяльністю [3].

Особливу цікавість користувачів в мережі Інтернет сьогодні привертають повідомлення в електронних ЗМІ та соціальних мережах. Зважаючи на це зазначені джерела перетворюються на потужний інформаційний ресурс, контентне наповнення якого охоплює практично усі прошарки цільової аудиторії. Залежно від того, як подається такий контент та який посил він несе у собі, можна визначити, чи він містить або ні загрози інформаційній безпеці держави, у тому числі й у воєнній сфері.

Отже, актуальність проблеми виявлення інформаційних загроз та деструктивних впливів не викликає сумнівів. Досвід АТО та ООС показав, що сьогодні перед органами військового управління, відповідальними за інформаційну безпеку держави у воєнній сфері, стоїть ряд важливих та складних завдань, одним з яких є визначення джерел воєнної небезпеки, встановлення характеру та ступеня воєнних загроз державі, а також факторів, що можуть вплинути на хід та результати збройного конфлікту.

Література

1. Вооруженные силы зарубежных государств: информационно-аналитический сборник / А.Н. Сидорин, Г.М. Мингатин, В.М. Прищепов, В.П. Акуленко. – М.: Воениздат, 2009. – 528 с.

2. Социальные сети: модели информационного влияния, управления и противоборства / Д.А. Губанов, ДА. Новиков, А.Г. Чхартишвили. – М.: ФИЗМАЛИТ, 2010. – 228с.

3. Основи стратегії національної безпеки та оборони держави: підруч. / О.П. Дузь-Крятченко, Т.М. Дзюба, А.О. Рось, ін. – 2-ге вид., доп. і випр. – К.: НУОУ, 2010. – 591 с.

УДК 355.451

Прокопенко Є.М.
кандидат технічних наук
Сівоха І.М.
Національний університет оборони України
імені Івана Черняховського

ПРІОРИТЕТИ РОЗВИТКУ СИСТЕМИ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ СЕКТОРА БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Розвиток системи стратегічних комунікацій сектора безпеки і оборони України є одним з ключових питань підготовки до оборони та забезпечення відсічі гібридної агресії.

Сучасні виклики для воєнної безпеки України обґрунтовують необхідність пошуку інструментарію, за допомогою якого стане можливою організація результативної взаємодії як в системі Міністерства оборони України, так і між структурами сектора безпеки і оборони (СБО) України. Потенцій-

ним інструментарієм такої взаємодії виступає система стратегічних комунікацій (ССК), яка дає можливість у межах діючих правових норм і принципів, організувати спільну відсіч гібридним операціям, які проводить агресор. Удосконалення ССК СБО є актуальною проблемою.

Проведений аналіз наукових розробок і діючих документів стратегічного і оборонного планування дозволяє стверджувати, що проблема стратегічних комунікацій СБО досліджена недостатньо, а функціонування ССК СБО вимагає удосконалення.

Метою є визначення та обґрунтування пріоритетів розвитку функціонування ССК СБО на основі застосування нових технологій стратегічних комунікацій.

Стратегічні комунікації є широкою за охватом діяльністю, яка включає питання спільної стратегії, корпоративних стандартів, регламентації взаємодії складових СБО на всіх ієрархічних рівнях управління, гармонізації дій в бойових, інформаційних, психологічних операціях, публічній дипломатії. Під ССК СБО будемо розуміти сукупність суб'єктів зі встановленими між ними зв'язками в єдиному інформаційному полі, стандарти і технології комунікацій, направлені на забезпечення воєнної безпеки України.

Технології стратегічних комунікацій мають універсальний характер і можуть бути застосовані у всіх сферах національної безпеки та на різних ієрархічних рівнях комунікаційної системи що в сукупності становить ССК.

Розглянемо напрями (технології) розвитку складових системи стратегічних комунікацій, які за думкою Центру стратегічних комунікацій НАТО, вимагають врахування при удосконаленні ССК з метою забезпечення воєнної безпеки.

Технології "м'яких" (soft) комунікацій направлені на забезпечення воєнної безпеки невійськовими інструментами та включають як стратегічні складові, так і комунікативні характеристики [1]. Комунікативною характеристикою виступає інверсія, яка проявляється в стратегічних наративах. Розвиток технологій комунікативних компонентів "м'яких" комунікацій "пов'язані" з використанням нових інформаційних технологій в різноманітних сегментах її практичного застосування. Це призводить до формування нових інформатизованих видів "м'яких" комунікацій: цифрова дипломатія, управління, розвідка тощо.

Технології "жорстких" (hard) комунікацій пов'язані із застосуванням військово-політичного або економічного примусу для корекції поведінки та інтересів інших сил. Технології включають примусову дипломатію, застосування або загрозу застосування воєнної сили, залякування і захист власних стратегічних інтересів, а також надання допомоги, хабарі, санкції та інтервенції. "Жорсткі" комунікації використовуються для визначення переговорного процесу, в якому застосовуються тиск і загрози як дієвого важеля.

Технології "інтелектуальних"*(smart) комунікацій* засновані на поєднанні силових спроможностей "жорстких" комунікацій та невоєнних спроможностей "м'яких" спроможностей для забезпечення воєнної безпеки. Така технологія акумулює в собі найбільш інформаційні, інтелектуальні і високотехнологічні інструменти впливу, використання яких характеризується системністю і раціональністю.

До "інтелектуальних" технологій стратегічних комунікацій відносяться рефлексивне управління, *sharp* та *blockchain*.

Технології, засновані на *рефлективному управлінні* - процесах передачі противнику спеціально підготовленої інформації з метою спонукати його на прийняття певних рішень в інтересах ініціатора процесу [2].

Окреме місце в системі стратегічних комунікацій займають технології позиційних (*sharp)* комунікацій, як сукупність узгоджених й взаємозв'язаних за метою, завданнями, місцем й часом одночасних і послідовних операцій інформаційного впливу та заходів кібернетичних атак, які проводяться в інформаційно-комунікаційному середовищі визначеної країни (регіоні) за єдиним замислом і планом для вирішення стратегічних завдань у встановлений період часу.

До технологій ССК СБО відносяться такі процедури, як моніторинг соціальних мереж, алгоритми виявлення недостовірної (фейкової) інформації, перевірка надійності джерел та використання різних методів оцінювання достовірності інформації. Разом з тим, проблема полягає не в розповсюдженні недостовірної інформації і спаму в ССК, а у технологіях, які спроможні відокремлювати недостовірну інформацію і спам. Для вирішення цієї проблеми використовуються процедури, які засновані на технології *блокчейну (Blockchain)* і відокремлюють надійні джерела інформації від недостовірних.

Основою для забезпечення процесів синхронізації застосування всіх технологій ССК СБО є єдиний інформаційний простір, який являє собою сукупність баз і банків даних, технологій їх ведення та використання, інформаційно-телекомунікаційних систем і мереж, що функціонують на основі єдиних принципів і за загальними правилами, що забезпечує інформаційну підтримку і взаємодію складових СБО.

Таким чином, організаційні структури СБО всіх рівнів, засоби та технології комунікацій утворюють інфраструктуру ССК СБО. Це вимагає від складових СБО міжвідомчої горизонтально-вертикально узгодженої та скоординованої комунікаційної діяльності, наявності спеціальних комунікаційних підрозділів і визначеного плану дій в комунікаційному просторі. Для результативної *протидії гібридним загрозам ССК СБО повинна бути* скоординована на всіх рівнях управління, спрямована на управління процесами прийняття рішень як всередині СБО, так і за його межами, з метою забезпечення адекватного реагування на гібридні загрози. Реалізація цих

функцій вимагає створення державного центру по боротьбі з дезінформацією і пропагандою. Головними завданнями нового органу повинні стати: аналіз інформаційного поля України, виявлення і локалізацію загроз і викликів системі політичних і ідеологічних орієнтирів суспільства, координацію пропагандистської діяльності, забезпечення своєчасного реагування на інформаційні операції і окремі акції. Частиною центру може стати бюро стратегічних комунікацій. Така структура на першому етапі буде орієнтована на моніторинг інформаційного простору, виявлення та оцінювання гібридних загроз в інтересах СБО України, а в перспективі розширить сферу своєї діяльності на стратегічні комунікації. Враховуючі перелік завдань, такому центру необхідно надати статус не тільки державного, а міжнародного спеціального органу, який візьме під управління і координацію роботу структур СБО з питань стратегічних комунікацій.

Література

1. Roselle L., Miskimmon A., O'Loughlin B. Strategic narrative: a new means to understand soft power // Media, War & Conflict. 2014. Vol. 7(1). P. 70–84.

2. Salnikova O.F., Sivoha I.M., Ivashchenko A.M. Strategic Communication in the Modern Hybrid Warfare. "Social Development & Security", 2019, Vol. 9 No 5. – P.133-142 DOI ID: 1033445/sds.2019.9.5.9.

УДК 378.1

Пучков О.О.
кандидат філософських наук, професор
Конюшок С.М.
кандидат технічних наук, доцент,
Інститут спеціального зв'язку та захисту інформації НТУ
«КПІ імені Ігоря Сікорського»

ОСВІТА І ПРОСВІТА У СФЕРІ КІБЕРБЕЗПЕКИ – ЗАВДАНЯ ПРОЄКТУ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ (2021–2025 РОКИ)

4 березня поточного року на веб-ресурсі Ради національної безпеки і оборони України оприлюднений проєкт Стратегії кібербезпеки України (2021 – 2025 роки) задля його громадського обговорення [1].

Серед загроз кібербезпеці в проєкті Стратегії, зокрема, виділяється "Зростання кіберзлочинності в національному сегменті кіберпростору є масштабною загрозою, яка завдає шкоди державним інформаційним ресурсам, суспільним процесам, особисто громадянам, що знижує довіру суспі-

льства до інформаційних технологій та призводить до значних матеріальних втрат... Ситуація ускладнюється через низький рівень кіберграмотності населення, зокрема пересічних користувачів електронних послуг" [2].

З метою набуття кіберстійкості національною системою кібербезпеки в проєкті Стратегії пропонується мінімізувати ризики, що пов'язані з вказаною загрозою, шляхом досягнення ряду стратегічних цілей, серед яких відзначимо: Ціль К.2. "Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки", яка, серед іншого декларує потребу "провести докорінну реформу системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки" та зазначає, що "кібергігієна, цифрові навички, кіберобізнаність щодо сучасних кіберзагроз та протидії ним мають стати невід'ємними елементами освіти кожного українського громадянина" [2].

Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського (далі – Інститут) має значний позитивний досвід у сфері підготовки кадрів та підвищення кваліфікації фахівців з кібербезпеки та кіберзахисту, а також в проведенні занять з кібергігієни [3].

Унікальність Інституту полягає в подвійному підпорядкуванні. З одного боку, Інститут є закладом освіти Держспецзв'язку, а з іншого боку, є військовим навчальним підрозділом технічного університету європейського зразка – КПІ ім. Ігоря Сікорського.

Підготовка фахівців в Інституті здійснюється за спеціальностями: 122 Комп'ютерні науки, 125 Кібербезпека, 172 Телекомунікації та радіотехніка за відповідними освітньо-професійними програмами на бакалаврському і магістерському рівнях та, за відповідними освітньо-науковими програмами, на освітньо-науковому рівні вищої освіти.

Наразі Інститут забезпечує підготовку офіцерських кадрів виключно за державним замовленням за очною (денною) формою навчання для потреб Держспецзв'язку, СБУ, СЗР та УДО. Крім того, в межах виконання міжнародної угоди у галузі підготовки фахівців із вищої освітою Інституту з 2007 року здійснює підготовку військовослужбовців Комітету Національної Безпеки Республіки Казахстан.

З огляду на значний досвід підготовки фахівців з вищою освітою в сфері захисту інформації, науково-педагогічні працівники Інституту ініціювали серію відкритих уроків, під час яких спільно з курсантами Інституту викладають інформацію щодо небезпек в кіберпросторі, а в підсумку надають рекомендації щодо мінімізації відповідних ризиків. Наприклад, в межах щорічної європейської традиції проведення в жовтні Місяцю кібербезпеки, який організовують Торгово-Промислова Палата України спільно з Держспецзв'язку, Інститутом проведені в закладах освіти України відкриті уроки на тему "Вступ до кібергігієни" [4].

Метою даної соціальної ініціативи є покращення розуміння питань кібергігієни, підвищення обізнаності про кіберзагрози та шляхи їх запобігання. З огляду на значний інтерес до заняття з боку педагогів і батьків учнів, прийнято рішення не обмежувати дану соціальну ініціативу одним місяцем та поширити її проведення на всю територію України.

Актуальність таких заходів полягає в тому, що сучасним учням старших класів притаманна висока самостійність і незалежність вибору інформаційних джерел в мережі Internet, одночасно з властивою підліткам цього віку емоційністю, вразливістю та схильністю до ідеалізації. Суміщення таких факторів робить підлітків надзвичайно вразливими до негативних інформаційних впливів, шахрайства та цькування.

Станом на сьогодні, за час проведення занять "Вступ до кібергігієни" охоплено близько 180 шкіл та ліцеїв України, а відкриті уроки змогли відвідати понад 10 000 учнів. В умовах карантину, наші фахівці перейшли до онлайн формату проведення занять.

Література

1. Робоча група при НКЦК РНБО України схвалила проєкт Стратегії кібербезпеки України. URL: https://www.rnbo.gov.ua/ua/Diialnist/4838.html (дата звернення: 10.03.2021).

2. Проєкт Стратегії кібербезпеки України (2021 – 2025 роки). URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 10.03.2021).

3. Щиголь Ю.Ф., Пучков О.О. Шляхи підвищення якості підготовки фахівців з кібербезпеки в інтересах сектору безпеки і оборони України. Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання : матеріали наук.-практ. конф., м. Київ. 18-19 листоп. 2020 р. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2020. С. 16.

4. Коляденко В.А., Конюшок С.М. Соціальна ініціатива Інституту спеціального зв’язку та захисту інформації КПІ ім. Ігоря Сікорського "Кібергігієна в школах України". Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання : матеріали наук.-практ. конф., м. Київ. 18-19 листоп. 2020 р. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2020. С. 184.

УДК 140.8
Романов М.С.
доктор юридичних наук,
старший науковий співробітник, доцент,
Національний університет «Острозька академія»

ЩОДО ЗАХОДІВ В УКРАЇНІ З ПРОТИДІЇ ГІБРИДНОМУ ВПЛИВУ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

За офіційними повідомленнями 11 березня Радою національної безпеки та оборони України створено ***Міжнародний центр протидії дезінформації.*** Який розгортає свою діяльність в Ситуаційному центрі Апарату Ради нацбезпеки та оборони України, який знаходиться на вулиці Банковій. Це давно очікуване рішення. В країні вкрай необхідний координуючий орган із протидії інформаційній складовій гібридного впливу Російської Федерації. Дуже важливо що для організації активної протидії дезінформації планується залучення спецслужб, про що повідомляв на брифінгу секретар РНБО Олексій Данилов [1]. У свою чергу Заступник голови Виконавчого Комітету реформ національної ради реформ Олександр Ольшанський уточнив, що цей центр координуватиме діяльність різних гілок влади та інших, серед інших – Міністерства культури та інформаційної політики, Інституту стратегічних досліджень, спецслужб [2]. Якщо так, то можна надіятись на наступальність у зазначеному, тобто не запізніло реагувати на прояви такого виду агресії, а через отримання інформації про наміри супротивника щодо організації і проведення акції інформаційно-психологічного впливу, самому організовувати упереджувальні заходи. Це один із показників наступальності.

Слід пам’ятати про те, що Міністерство інформаційної політики нині в «Бозі спочиле». Натомість - це окремий Департамент в Міністерстві культури і інформаційної політики. За даними у відкритих джерел зараз у Міністерстві створюється інший ***Центр протидії дезінформації***. Про це повідомив міністр Олександр Ткаченко 16 лютого під час онлайн-семінару «Протидія дезінформації: європейські підходи та стандарти». Зазначений Центр «у співпраці з українськими неурядовими організаціями буде протистояти російській пропаганді». Водночас, появилась інформація про створення іншої структури в Міністерстві - ***Центру стратегічних комунікацій та інформаційної безпеки.***

З урахуванням відсутності інформації щодо Положення про ці, схожі структури, не має можливості надавати характеристику перспективам їх діяльності, але насторожує можливі напрями паралелізму в роботі близьких за функціями структур в цьому Міністерстві.

Як вбачається то функція Міжнародного центру протидії дезінформації при РНБО більш глобальна. Насамперед, вона має координувати діяльність з протидії інформаційній агресій на міждержавному рівні. Так наприклад Національний університет «Острозька академія» є співучасником міжнародного проекту Європейського Союзу Еразмус+ WARN – Академічна протидія гібридним загрозам (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP. У рамках зазначеного розробляються новітні підходи участі ЗВО у заходах із протидії гібридному впливу РФ насамперед інформаційному. Національна академія СБ України запрошена до цього проекту. Мають місце інші проекти в інших міністерствах з цього напрямку. То, думаю, насамперед можна розглянути питання щодо організації об'єднавчого форуму у процесі якого організаційно визначитись із складом таких структур, що уже здійснюють заходи із протидії інформаційному впливу. Для прикладу такими структурами є організаціями що займаються фактчекінгом в Україні є StopFake, VoxUkraine, FactCheck та «Слово і діло». Та інші. Сюда можна внести і структури із ЗВО наприклад НУ ОА, НА СБ України. Тут можна назвати позитивний досвід Національної академії сухопутних військ імені гетьмана Петра Сагайдачного. Із курсантів створено молоду команду, яка займається висвітленням найцікавішої та актуальної інформації про Україну та її захисників, а також намагатиметься розвіювати російські фейки та міфи ворожої пропаганди. Так курсанти цього навчального закладу долучилися до міжнародного проєкту Peer-to-Peer (колегіальне навчання), аби протистояти російській пропаганді та дезінформації. Організований цей проєкт і відбувається під егідою компанії EdVenture Partners (EVP) головною метою є здобуття нового досвіду, вмінь і навичок.

Література

1. Брифінг Данілова за результатами засіадння РНБО / [Електронний ресурс]. - Режим доступу: URL: https://www.ukrinform.ua.

2. РНБО створила Міжнародний центр протидії / [Електронний ресурс]. - Режим доступу: URL: https://www.ukrinform.ua.

3. Матеріали онлайн-семінару «Протидія дезінформації: європейські підходи» / [Електронний ресурс]. - Режим доступу: URL: https:// www.eeas.europa.eu.

4. Офіційний сайт Національної академії сухопутних військ імені гетьмана Петра Сагайдачного [Електронний ресурс]. - Режим доступу: URL: https://www.asv.gov.ua.

УДК 351.86
Сальнікова О.Ф.
доктор наук з державного управління,
старший науковий співробітник
Іжутова І.В.
Національний університет оборони України
імені Івана Черняховського

АКТУАЛЬНІ ПРОБЛЕМИ РОЗВИТКУ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасна інформаційна епоха, інформаційний прогрес змінюють умови існування людини, а питання інформаційної безпеки в умовах стрімкого цифрового розвитку стає дедалі актуальнішим. Відбувається перенесення полю бою в інформаційну площину, збільшення кількості поширення недостовірної інформації, дезінформації та інформації маніпулятивного характеру, важливим фактором впливу та зміни системи національної безпеки є всесвітня пандемія, яка провокує розвиток інфодемії. А доступні нові технології роблять сучасну людину вразливішою, відповідно, впливаючи на всю систему. Так, у Воєнній доктрині України, затвердженій Указом Президента України від 24 вересня 2015 року № 555/2015 [1], з'явилося визначення "стратегічні комунікації" (далі – "СК") 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. Це певна філософія, яка забезпечує комплексну відповідь на сучасні виклики та загрози.

У Стратегії національної безпеки України, прийнятої минулого року, визнано, що "деструктивна пропаганда як ззовні, так і всередині України, використовуючи суспільні протиріччя, розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність, крім того, наголошено на відсутності цілісної інформаційної політики держави і слабкості системи стратегічних комунікацій, що ускладнює нейтралізацію цієї загрози. Тому визначено, що Україна розвиватиме інклюзивний політичний діалог через створення системи стратегічних комунікацій" [2].

Залежність сучасного світу від інформації та легкого її донесення до споживачів вимагає посилення відповідальності за поширення недостовірних даних, надання ефективного інструментарію для перевірки інформації, формування стійкого суспільства, що дозволить забезпечити належний рівень інформаційної безпеки. Одним із таких інструментаріїв є анонсування створення міжнародного центру протидії дезінформації [3].

Література

1. Указ Президента України Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року “Про нову редакцію Воєнної доктрини України”. URL: https://zakon.rada.gov.ua/laws/show/555/2015#Text.

2. Указ Президента України №392/2020 Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року “Про Стратегію національної безпеки України”. URL: https://www.president.gov.ua/documents/3922020-35037.

3. Центр протидії дезінформації, анонсований Президентом України, буде презентовано у четвер, 11 березня. 10.03.2021. URL: https://ua.interfax.com.ua/news/general/729098.html [дата звернення: 10.03.2021].

УДК 004.94.355

Самчишин О. В.
кандидат технічних наук
Носова Г. Д.
Житомирський військовий інститут імені С. П. Корольова

ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

Розвиток та впровадження інформаційних технологій в усі сфери життєдіяльності суспільства потребує постійного забезпечення кібернетичної безпеки як невід’ємної складової національної безпеки держави. Особливо актуальним є забезпечення кібернетичної безпеки в умовах ведення гібридних війн у сучасних збройних конфліктах. Для підвищення обороноздатності та забезпечення національних інтересів у кіберпросторі збройні сили (ЗС) розвинених держав світу проводять комплекс організаційних та технічних заходів, спрямованих на оперативне адекватне реагування на виклики та загрози у кіберпросторі.

Близько 60 країн мають власні системи кібербезпеки (кібервійська), які створені за останнє десятиріччя. Усі ці підрозділи призначено для ведення кібернетичної боротьби – комплексу заходів, спрямованих на здійснення управлінського і/або деструктивного впливу на автоматизовані ІТ-системи протиборчої сторони та захисту від такого впливу власних інформаційно-обчислювальних ресурсів завдяки використанню спеціально розроблених програмно-апаратних засобів, а також проведенню системи спеціалізованих навчань. Тому питання всебічного аналізу сучасного стану системи кібернетичної безпеки держави та надання пропозицій щодо удосконалення потенціалу сектора безпеки та оборони України в сфері кібербезпеки має актуальний характер.

Гібридна війна, яка відбувається між Росією і Україною, включає не тільки воєнні дії та інформаційно-психологічні операції, а й кібернетичні атаки. Підтверджено факти використання шкідливого та вірусного програмного забезпечення (контенту) Turla/Uroburos/Snake, RedOctober, MiniDuke та NetTraveler. Протягом усього конфлікту відмічається активність анонімних користувачів чи проросійських активістів, які шляхом проникнення в інформаційні мережі розповсюджують "фейкову" інформацію.

Основними об'єктами кібернетичних атак залишаються атомні електростанції; об'єкти критичної інфраструктури в енергетичній, соціальній та банківській сферах (лікарні, транспортні компанії, фінансові установи, сервісні служби тощо); системи відеонагляду типу "безпечне місто; інформаційно-телекомунікаційні системи органів влади; інші об'єкти критичної інфраструктури. Крім того, досвід останніх років свідчить про успішне проведення кібератак на навігаційне обладнання аеропортів, інформаційно-комунікаційні системи медичних установ, обладнання цифрового зв'язку мобільних операторів та провайдерів Інтернету тощо. Такі можливості кіберзброї здатні вивести світовий тероризм та гібридну агресію РФ проти України на новий рівень, де ніхто не буде застрахований від неконтрольованих техногенних та соціотехнічних катастроф.

З метою протидії новим загрозам та викликам на фоні активної агресії РФ у кіберпросторі Україна продовжує створення повноцінної системи національної кібернетичної безпеки. Робочою групою при НКЦК РНБО України було схвалено проєкт Стратегії кібербезпеки України на 2021–2025 роки, метою якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства, держави. Новацією Стратегії є визначення механізмів її реалізації та критеріїв вимірювання успіхів на цьому шляху. Передбачається, що у перший рік дії Стратегії будуть невідкладно розроблені індикатори оцінки стану кібербезпеки і кіберзахисту; проведено огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом; розроблені та запроваджені механізми проведення оглядів стану національної системи кібербезпеки. Показниками для розробки таких індикаторів мають стати сучасні виклики у цій сфері, зокрема такі як: активне використання кіберзасобів у міжнародній конкуренції за світове лідерство; мілітаризація кіберпростору та зростаючі технологічні можливості кіберзброї; зростання технологічного рівня протиправних посягань на інтереси держави, суспільства та окремих громадян із застосуванням методів соціальної інженерії, використання технологій штучного інтелекту та криптотехнологій; вплив на економічну діяльність та соціальну поведінку поширення пандемії COVID-19.

З огляду на викладене вище, пріоритетами забезпечення кібербезпеки України є: убезпечення кіберпростору задля захисту суверенітету держави

та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки.

Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації Стратегії, а саме: дієва кібероборона; посилення спроможностей у протидії розвідувально-підривній діяльності у кіберпросторі та кібертероризму; посилення спроможностей у протидії кіберзлочинності; розвиток асиметричних інструментів стримування.

Література

1. Стратегія кібербезпеки України (2021 – 2025 роки) Проєкт. Режим доступу – https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/.

2. Косогов О. М., Сірик А. О. Основні проблемні питання та напрямки підвищення ефективності державної інформаційної політики України в умовах гібридної війни / Київ: НУОУ імені І. Черняховського, 2017. 104 с.

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
імені Івана Черняховського

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ В СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ У ВОЄННІЙ СФЕРІ

Державна політика України у сфері інформаційної безпеки спрямована на накопичення та захист національних інформаційних ресурсів, розробку та впровадження сучасних безпечних інформаційних технологій, побудову захищеності інформаційної інфраструктури. Разом з тим, серед численних наукових праць, присвячених захищеності інформаційних ресурсів, незважаючи на їх незаперечну актуальність, на жаль, не приділено достатньої уваги розкриттю сутності, ролі та місця захищеності інформаційних ресурсів в сучасних умовах, дослідженню їх основних характеристик; бракує системності в розгляді цього питання.

Визначальної ваги інформаційна безпека набуває у воєнній сфері. При цьому під інформаційною безпекою держави у воєнній сфері розуміється

стан захищеності інформаційного простору воєнної сфери в умовах впливу внутрішніх та зовнішніх інформаційних загроз. У воєнній сфері захист інформаційних ресурсів є основою обороноздатності країни, безпосередньо пов'язаний із забезпеченням інформаційної безпеки сектору безпеки і оборони.

Взагалі, під *інформаційним ресурсом слід розуміти факти, відомості, дані й саму інформацію, відмінною і невід'ємною характеристикою яких є їх прагматична цінність, що визначається практичними потребами в інтересах вирішення певних завдань.*

Відомо, що інформаційною загрозою є можлива подія, дія, процес або явище, що може прямо чи опосередковано нанести збитки інформаційним ресурсам системи шляхом розкриття або руйнування даних. Внаслідок реалізації противником загрози можуть постраждати об'єкти інфраструктури та наявні інформаційні ресурси воєнної сфери, що складають основу інформаційного забезпечення системи державного та військового управління.

Результатом реалізації інформаційної загрози може бути:

руйнування об'єкта (засобів, даних, обладнання, зв'язку);

ушкодження об'єкта (даних);

видалення або втрата об'єкта (обладнання, даних);

розкриття об'єкта (даних);

використання або впровадження нелегального об'єкта (обладнання, програмного забезпечення, фальшивих даних).

Навмисну реалізацію інформаційної загрози називають інформаційною атакою, яка часто-густо спрямована противником на інформаційні ресурси воєнної сфери. Саме у військовій справі наявність інформаційних ресурсів все більшою мірою обумовлює оперативність прийняття управлінських рішень, структуру органів управління, військ (сил), якість та кількість озброєння та військової техніки, оцінку рівня їх достатності, ефективність дій збройних сил, застосування озброєння і, в підсумку, результат збройного протистояння. Тому захист інформаційних ресурсів – одне із пріоритетних завдань інформаційної безпеки України, є важливою складовою державної інформаційної політики, зокрема у воєнній сфері.

Актуальними загрозами інформаційній безпеці України у воєнній сфері є:

здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу ЗС України та інших військових формувань;

недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

інформаційне домінування держави-агресора на тимчасово окупованих територіях;

неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, недостатній рівень медіа-культури суспільства.

Виходячи із зазначених загроз, сутність інформаційного забезпечення системи управління, зокрема у воєнній сфері, повинна полягати у забезпеченні процесу ефективного формування та використання інформаційного ресурсу воєнної сфери в інтересах виконання завдань сектором безпеки і оборони (захисту національних інтересів України від зовнішніх інформаційних загроз).

Таким чином, пропонується наступне визначення: *захист інформаційних ресурсів воєнної сфери – сукупність правових, адміністративних, організаційних, технічних та інших заходів сектору безпеки та оборони, що забезпечують збереження, цілісність інформації (інформаційних ресурсів воєнної сфери) та належний порядок доступу до неї (них)*.

Запропоноване визначення захисту інформаційних ресурсів в системі управління воєнної сфери розкриває сутність інформаційної функції щодо захисту інформаційних ресурсів у загальному контурі державного військового управління.

Отже, одним з актуальних питань МО України та ЗС України щодо створення дієвого інформаційного забезпечення системи державного управління у воєнній сфері є впровадження всебічного захисту інформаційних ресурсів для ефективного функціонування сектору безпеки і оборони.

УДК 355.40:358.12

Сергієнко О.П.
Військова частина А0987

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Враховуючи розвиток інформаційних технологій в світі й значний науково-технічний та фаховий потенціал вітчизняних виробників, необхідним шляхом подолання сучасних викликів є створення цілісного комплексу захищеної інформаційної інфраструктури в сфері оборони.

Головною задачею такого комплексу є оперативне надання суб'єктам прийняття рішень вичерпної, актуальної, своєчасної й вірогідної інформації щодо стану військ та їх всебічного ресурсного забезпечення шляхом постійної інформаційно-аналітичної підтримки процесів управління оборонними ресурсами. За визначенням – інформаційна інфраструктура об'єкту є

системою організаційних структур, систем, які забезпечують функціонування та розвиток інформаційного простору цього об'єкту та включають в себе сукупність інформаційних центрів, систем, банків даних і знань, апаратно-програмних засобів, і технологій збору, зберігання, обробки та передачі інформації для надання доступу користувачам до інформаційних ресурсів щодо визначеного об'єкту. Технічною основою системи управління оборонними ресурсами повинна стати мережа ситуаційних центрів, об'єднаних між собою системою телекомунікацій, яка б забезпечувала потреби Збройних Сил України в єдиному масштабованому, високонадійному обчислювальному ресурсі Інтелектуально-технологічною основою такої системи повинно стати відповідне системне та прикладне програмне забезпечення, сукупність інформаційно-аналітичних систем та баз даних з технологіями їх обробки на основі сучасних технологій з використанням віртуалізації ресурсів, "хмарних" та ГІС-технологій.

Комплексне дослідження існуючих складових інформаційної безпеки держави у воєнній сфері [1; 2] показало, що основні складові повинні реалізувати повноцінну інформаційну інфраструктуру для надання керівництву ЗС України і держави та органам військового управління послуг із централізованих сервісів доступу, збереження, обробки і обміну інформацією та засобами транспортування і захисту інформації. Аналіз систем управління військовими ресурсами в країнах НАТО свідчить про те, що оборонні відомства і збройні сили шукають шляхи підвищення ефективності використання оборонних ресурсів за рахунок постійного аналізу ситуації у сфері безпеки та підготовки політико-стратегічних рішень як підґрунтя процесу управління оборонними ресурсами.

З іншого боку, цей процес потребує постійного зворотного зв'язку, щоб військово-політичні задуми забезпечувалися відповідними можливостями збройних сил і достатніми ресурсами для їх виконання. Зазначений принцип реалізовано в загальній концепції альянсу CALS - 61 Continuous Acquisition and Life-cycle Support (Постійна підтримка створення та життєвого циклу) – яка визначає розробку плану інформаційного менеджменту протягом всього життєвого циклу оборонних продуктів (систем).

Тому метою тез доповіді є визначення шляхів підвищення ефективності захисту об'єктів інформаційної інфраструктури держави.

Враховуючи положення державної політики поглиблення співпраці з Організацією Північноатлантичного договору, з метою досягнення критеріїв, необхідних для набуття членства у цій організації, можна визначити три глобальних принципа створення захищеної інформаційної інфраструктури сфери оборони: - дотримання національних інтересів та законодавства України; - дотримання законів життєвого циклу ІТ-систем; - дотримання стандартів НАТО [3].

Головною метою функціонування захищеної інформаційної інфраструктури Збройних Сил України є оперативне надання суб'єктам прийняття рішень вичерпної, актуальної, своєчасної й вірогідної інформації щодо стану військ та їх всебічного ресурсного забезпечення шляхом постійної інформаційно-аналітичної підтримки процесів управління оборонними ресурсами. Розподілена база даних АСУ військами є елементом інформаційної інфраструктури Збройних Сил України. Представляє собою децентралізовану розподілену інформаційну систему, в якій сервера баз даних знаходяться на окремих вузлах (починаючи з бригади (полку) і вище), а інформація посадовим особам повинна бути доступною у визначені терміни не зважаючи на вплив дестабілізуючих факторів.

Середню швидкість передачі інформації визначають на основі даних статистики спостереження і використовують для подальшої оцінки витрат часу на переміщення фрагмента даних. Оцінка витрат на підтримку копії фрагмента даних проводиться на основі використовуваних систем управління базами цих протоколів актуалізації.

Отже, з-поміж загроз критичній інфраструктурі держави називають пандемії, промислові аварії, терористичну та злочинну діяльності, кібератаки, стихійні лиха. Держава має забезпечувати захист об'єктів критичної інфраструктури від усіх суттєвих загроз, які можна віднести до трьох категорій: техногенні, природного характеру та соціально-політичні.

Література

1. Бірюков, Д. С. Зелена книга з питань захисту критичної інфраструктури в Україні [Текст] /Д. С. Бірюков, С. І. Кондратов, О. М. Суходоля. – К.: НІСД, 2015.

2. Paul Ch. Strategic Communication: Origins, Concept, and Current Debates. Santa Barbara, 2011.;Tatham S.A. Strategic Communication: A Primer Academy of the United Kingdom, 2008.

3. Tatham S.A. Strategic Communication: A Primer Academy of the United Kingdom, 2008.

УДК 04.946.5

Скачек Л.М.
кандидат технічних наук, доцент,
Національна академія внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Поняття "національна безпека" має велику кількість вимірів та аспектів, різниця між якими полягає в тому числі і у відповідних позиціях, з яких

розглядається це питання. Навіть при наявності певних принципових узгоджень щодо методології та системи світогляду відразу будуть помітні розбіжності в баченні сутності та змісту національної безпеки у фахівців - правників на відміну від військових, економістів, політологів тощо.

По-перше, це теоретична сфера національної безпеки, яка розглядає названу проблему в площині розуміння змісту та сутності, визначення її місця в системі державної діяльності тощо.

По-друге, це практична сфера національної безпеки, до якої відносять нормативно-правові основи діяльності держави, спрямованої на захист національної безпеки та на створення відповідних дієвих механізмів цього захисту.

Згідно ст. 1 Закону України "Про національну безпеку України" національні інтереси - це життєво важливі матеріальні, інтелектуальні і духовні цінності Українського народу, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток. Але, разом з тим, залишається відкритим питання про конкретні механізми та принципи визначення змісту національних інтересів.

Так, наприклад, Рада національної безпеки і оборони України згідно ст. 107 Конституції України є "координаційним органом з питань національної безпеки і оборони при Президентові України", який "координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони".

Закон України "Про Раду національної безпеки і оборони України" ці повноваження значно розширює. Згідно зі ст. 4 Закону "Про Раду національної безпеки і оборони України", Рада національної безпеки і оборони України: "розробляє та розглядає на своїх засіданнях питання, які відповідно до Конституції та законів України, Концепції (основ державної політики) національної безпеки України, Воєнної доктрини України належать до сфери національної безпеки і оборони та подає пропозиції Президентові України щодо: *визначення стратегічних національних інтересів України* ...".

Ще одним аспектом, який є критичним для визначення основних напрямків політики національної безпеки України, повинна бути адекватність цієї політики реальному місцю і ролі України у світових політичних та економічних процесах. Тим самим обумовлюється глобалізація і самозростання всього, що пов’язано з національними інтересами, національною безпекою.

Шукаючи свої власні виміри національної безпеки Україні слід орієнтуватися на країни іншого порядку, такі, що можуть бути зіставлені з Україною у відповідності до їх місця і ролі в світових процесах. Останнім часом нерідко наголошується на певній схожості геополітичного становища України та Канади.

Тобто, національна безпека це не самоціль, а лише засіб попередження чи подолання загроз реалізації цілей держави. В такому ж ракурсі повинна розглядатись сутність її інформаційного чинника.

Інформаційна безпека виступає невід'ємною складовою національної безпеки. Але, розглядаючи проблему інформаційної безпеки, необхідно брати до уваги той факт, що вона є досить специфічним видом безпеки.

Ця специфіка пов'язана, передусім, зі специфічним предметом цього роду безпеки - інформацією, сутність і природа якої ще й досі залишається предметом дискусій.

Література

1. Конституція України // Відомості Верховної Ради України. – 1996. – № 30. – 141 с.

2. Про національну безпеку України : Закон України // Відомості Верховної Ради. – 2018. – № 31. – 241 с.

3. Про Раду національної безпеки і оборони України // Відомості Верховної Ради України. – 1998, № 35 ст.237.

УДК 355.40

Сніцаренко П.М.
доктор технічних наук, старший науковий співробітник
Саричев Ю.О.
кандидат технічних наук, старший науковий співробітник
Грицюк В.В.
Національний університет оборони України
імені Івана Черняховського

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ЯК ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВОЄННІЙ СФЕРІ

У XXI столітті безпека інформаційного середовища стала найвагомішим фактором в усіх сферах національної безпеки. Її забезпечення значною мірою сприяє досягненню успіху у виконанні завдань в політичній, воєнній, економічній, соціальній та інших сферах державної діяльності.

Визначальної ваги інформаційна безпека набуває у воєнній сфері. До найважливіших категорій інформаційної безпеки у воєнній сфері відносяться:

інформаційний простір воєнної сфери – інтегроване інформаційне середовище, що створюється інформаційною інфраструктурою сектора безпеки і оборони;

інформаційна інфраструктура воєнної сфери – сукупність різноманітних інформаційних (автоматизованих) систем, телекомунікаційних мереж і

каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування у воєнній сфері;

інформаційний ресурс воєнної сфери – наявний обсяг даних та інформації, доступних для елементів інформаційної інфраструктури сектора безпеки і оборони в інтересах здійснення її суб'єктами функцій управління.

В сучасному цивілізованому світі проблема безпеки інформаційних ресурсів є надзвичайно актуальною. Розуміння проблеми захисту інформаційних ресурсів воєнної сфери в усій її багатогранності, оперативне виявлення та врахування недоліків захисних механізмів, передбачення можливих наслідків від реалізації інформаційних загроз, впровадження апробованих методів і надійних засобів сприятиме захисту інформаційних ресурсів воєнної сфери від небажаних впливів.

Таким чином, інформаційний ресурс серед основних об'єктів забезпечення інформаційної безпеки держави у воєнній сфері займає важливе місце, а його захист, серед іншого, є основою обороноздатності країни. Цілком очевидно, що будь-які заходи, які здійснюються, особливо в умовах бойових дій, без надійного захисту інформаційних ресурсів приречені на невдачу.

Певні аспекти захисту інформаційних ресурсів розглядали у своїх роботах чимало вчених. Водночас, незважаючи на незаперечну цінність цих праць, в них не приділено достатньої уваги розкриттю сутності, ролі та місця захищеності інформаційних ресурсів воєнної сфери в сучасних умовах, дослідженню їх основних характеристик; бракує системності в розгляді цього питання.

Взагалі, під *інформаційним ресурсом слід розуміти факти, відомості, дані й саму інформацію, відмінною і невід'ємною характеристикою яких є їх прагматична цінність, що визначається практичними потребами в інтересах вирішення певних завдань.*

Водночас, чинне законодавство не встановлює повного юридичного трактування складових інформаційного ресурсу, зокрема у воєнній сфері. Не визначені критерії віднесення інформаційного ресурсу до категорії державних та недержавних. Таке становище створило і надалі створюватиме труднощі щодо формування системи національних та відомчих інформаційних ресурсів, управління цією системою, а також правового оформлення функцій, пов'язаних з володінням, використанням інформаційним ресурсом та його розпорядженням.

Під інформаційною загрозою розуміють наміри, дії або явища, які шляхом інформаційного впливу на соціальні об'єкти, інформаційну інфраструктуру та інформаційні ресурси можуть ускладнити (унеможливити) реалізацію національних інтересів держави (функцій її структурних органів).

Внаслідок реалізації інформаційної противником можуть постраждати наявні інформаційні ресурси. Результатом реалізації інформаційної загрози може бути:

руйнування об'єкта (засобів, даних, обладнання, зв'язку);

ушкодження об'єкта (даних);

видалення або втрата об'єкта (обладнання, даних);

розкриття об'єкта (даних);

використання або впровадження нелегального об'єкта (обладнання, програмного забезпечення, фальшивих даних).

Навмисну реалізацію інформаційної загрози пов'язують з інформаційною атакою. Під *інформаційною атакою розуміють сукупність декількох короткочасних узгоджених за метою і часом інформаційних заходів, спрямованих на втручання в процес функціонування визначених об'єктів інформаційної інфраструктури.*

Узагальнений сценарій інформаційної атаки можна подати у вигляді наступних кроків: розвідка; вибір (або розробка) програми інформаційної атаки; злом цільової системи (читання, копіювання, знищення даних); завантаження "корисного вантажу" (яким, як правило, є шкідлива інформаційна програма); приховування слідів злому. Звичайно, послідовність може бути інша або можуть бути виключені окремі кроки даного сценарію.

Отже, сутність забезпечення інформаційної безпеки держави у воєнній сфері, системоутворюючим ядром якої є інформаційна інфраструктура МО України та ЗС України, полягає у забезпеченні процесу ефективного формування та використання національного інформаційного ресурсу в інтересах виконання завдань сектором безпеки і оборони України.

Таким чином, одним з актуальних питань МО України та ЗС України є впровадження всебічного захисту інформаційних ресурсів воєнної сфери від інформаційних загроз для ефективного функціонування сектору безпеки і оборони України.

УДК 321.011:65.012.8

Солодка О. М.
кандидат юридичних наук,
старший науковий співробітник,
Національна академія Служби безпеки України

ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ ДЕРЖАВИ – ІМПЕРАТИВ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Двома ключовими характеристиками сучасного історичного періоду є глобалізація та розвиток інформаційно-комунікаційних технологій, що

призвело до формування нового типу суспільного устрою – інформаційного суспільства, яке існує і розвивається на двох рівнях – національному та міжнародному. Відповідно, засоби забезпечення державного суверенітету в інформаційній сфері у різний спосіб впливають на розвиток національного і глобального інформаційного суспільства.

У першому випадку забезпечення державного суверенітету не вступає у безпосередній конфлікт з національним інформаційним суспільством, адже його розвиток на рівні держави (належний рівень правового забезпечення інформаційної сфери, вітчизняні інформаційні технології, національна ідеологія, медіаграмотність, критичне мислення тощо) сприяє забезпеченню інформаційного суверенітету. У другому випадку забезпечення державного суверенітету в інформаційній сфері та розвиток глобального інформаційного суспільства – майже взаємовиключні завдання, що обумовлено фактичною неможливістю окремої держави зберігати контроль над інформаційним простором в умовах високої інтеграції в глобальний інформаційний простір.

Отже, заходи, спрямовані на забезпечення державного суверенітету, можуть призводити до стримування процесів, спрямованих на розвиток інформаційного суспільства в контексті процесів глобалізації. З розвитком інформаційного суспільства також посилюються загрози державному інформаційному суверенітету як основоположного елементу інформаційної безпеки держави.

При цьому у світовій практиці, фактично реалізуються дві концепції забезпечення інформаційного суверенітету:

- адміністративна - жорстке ідеологічно задане державне регулювання доступу в інформаційний простір країни (Китай, Росія). Ця концепція визначається як «суверенітет кордонів», тобто контроль і обмеження з боку держави над потоками інформації і інфраструктурою, що їх забезпечують;

- ліберальна – законодавчо регламентоване забезпечення свободи інформації в поєднанні з кримінально-правовим та адміністративно-правовим захистом від екстремізму, тероризму, порнографії, порушення авторських прав (США, країни Євросоюзу). Ця концепція визначається як «суверенітет через експансію», адже Експансію здійснюють країни, які прагнуть «величі», тобто в контексті інформаційному – це країни інфолідери (Росія, США, Китай або об'єднання країн – ЄС).

Вище викладене актуалізує питання забезпечення інформаційного суверенітету в контексті міжнародної співпраці. Загалом експерти розрізняють чотири можливі шляхи розвитку правового регулювання інформаційного простору[1]:

- «Доктрина абсолютної свободи», яка відкидає ідею регулювання інтернет-ЗМІ та ЗМК, популярна передусім серед інтернет-користувачів. Во-

дночас, відкритий доступ до ресурсів глобального інформаційного суспільства має регулюватися з метою попередження зловживань, адже відсутність регуляторного механізму провокує ризики обмеження доступу до інформації та комунікації.

- «Саморегулювання» – на користь цього підходу висловлюються переважно ІТ-компанії та виробники контенту, які вбачають у ньому передусім вирішення проблем, пов'язаних з образливим контентом та захистом прав користувачів. Втім, зважаючи на гостру проблематику захисту авторських прав та електронної торгівлі, навіть за умов саморегулювання існує необхідність у створенні впорядкованої правовими нормами структурованої мережі, в рамках якої відбувалася б комунікативна активність;

- «Закритий клуб» – цей підхід спрямований на заповнення прогалин у національному законодавстві, пов'язаних із вирішенням регуляторних питань. Зокрема, відповідні рішення розробляються в рамках Організації економічної співпраці та співробітництва (ОЕСР), Великої вісімки (G8), СОТ, а також новими інституціями, що формуються в корпоративному секторі. Ризики такого підходу полягають у тому, що найбільш сильні економічно та розвинуті в технологічному плані суб'єкти можуть диктувати правила гри усім іншим, а ЗМІ та ЗМК сприйматимуться як бізнес, засоби розваги та тотального контролю над інформаційними ресурсами;

- Інституційний підхід, підґрунтям якого є демократизація глобального управління, що знаходить своє відображення в окремих ініціативах ООН та концепції «космополітичної демократії», який реалізується у процесах на зразок Всесвітнього саміту з інформаційного суспільства (ВСІС) і передбачає багатосторонню участь всіх зацікавлених суб'єктів у вирішенні питань, що їх безпосередньо стосуються, можуть стосуватися у майбутньому, або на їх власне переконання, є такими, що можуть прямо чи опосередковано зачіпати їх інтереси.

Отже, забезпечення інформаційного суверенітету держави в контексті розвитку інформаційного суспільства має забезпечувати досягнення балансу між збереженням національної ідентичності, національних інформаційних ресурсів, зниженням уразливостей критичної інформаційної інфраструктури, протидією шкідливим інформаційним впливам тощо та відкритістю й інтегрованістю держави до глобального інформаційного простору.

Література

1. Інтеграція України в Європейське інформаційне суспільство. Виклики і завдання. Київ. 2014. 260 с.

УДК 343.13
Тимофеєв А.О.
Інститут підготовки юридичних кадрів для СБУ
Національного юридичного університету ім. Я. Мудрого

ЕЛЕКТРОННЕ ДОСУДОВЕ РОЗСЛІДУВАННЯ ЯК ОДИН З НАПРЯМКІВ РОЗВИТКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Відповідно до ст. 2 КПК України завданнями кримінального провадження є захист особи, суспільства та держави від кримінальних правопорушень, охорона прав, свобод та законних інтересів учасників кримінального провадження, а також забезпечення швидкого, повного та неупередженого розслідування і судового розгляду з тим, щоб кожний, хто вчинив кримінальне правопорушення, був притягнутий до відповідальності в міру своєї вини, жоден невинуватий не був обвинувачений або засуджений, жодна особа не була піддана необґрунтованому процесуальному примусу і щоб до кожного учасника кримінального провадження була застосована належна правова процедура.

На сьогоднішній день виконання даних завдань здійснюється, зокрема, шляхом змішаного, частково електронного кримінального процесу. Так, відповідно до ст. 214 КПК, початок кримінального провадження суто електронний, а саме, внесення відомостей до Єдиного реєстру досудових розслідувань (далі – ЄРДР) з подальшим автоматичним формуванням електронного процесуального документа – витягу з ЄРДР. Проте, надалі досудове розслідування майже повністю йде паперовим шляхом. Відповідно до Наказу Офіса Генерального прокурора №298 від 30.06.2020 року «Про затвердження положення про ЄРДР, порядок його формування та ведення» до ЄРДР вноситься лише певна інформація про вчинення основних процесуальних дій, інша ж інформація відносно руху кримінального провадження та вчинених слідчих, розшукових, процесуальних дій існує виключно в паперовому форматі.

Відповідно до ст. 103 КПК України процесуальні дії під час кримінального провадження можуть фіксуватись виключно в певній фізичній формі, а електронна форма кримінального провадження не передбачена. До того ж існує стала практика ВС України (Постанови ВС у справах № 754/7062/15-к, № 761/20108/15-к, № 235/6337/18 та ін) відповідно до якої рішення в рамках досудового розслідування приймається у формі постанови і внесення відомостей до ЄРДР в електронній формі не може означати прийняття того чи іншого процесуального рішення без існування паперового документу, який це підтверджує.

Дані факти підтверджують, що впровадження в нашій країні електронного досудового розслідування можливе лише після внесення ґрунтовних

змін до вітчизняного законодавства, зокрема, в частині електронних доказів, прийняття процесуальних рішень в електронній формі та інших.

При цьому електронне досудове розслідування вирішило б ряд проблем, з якими стикаються всі сторони кримінального процесу, а саме:

- відносно сумнівів з приводу оригінальності процесуальних документів, у зв'язку з неможливістю їх зміни після внесення відомостей до реєстру;
- зменшення кількості паперових документів, що призведе до пришвидшення та здешевлення кримінального процесу;
- швидкої взаємодії між органами, закладами та установами, з метою отримання інформації необхідної для проведення досудового розслідування;
- збереження матеріалів кримінальних проваджень в належному стані для подальшого судового розгляду;
- швидкої взаємодії між всіма сторонами кримінального провадження, шляхом можливості подачі заяв, клопотань та надіслання повідомлень в електронній формі.

На даний момент існує досить таки великий іноземний досвід в запровадженні та здійсненні електронного досудового розслідування та електронного правосуддя. Так, Кримінально-процесуальний кодекс Естонії визначає широкий спектр процесуальних інструментів і процедур, що становлять електронний сегмент кримінального провадження, в тому числі електронну комунікацію між суб'єктами кримінального провадження. В деяких державах уже сьогодні матеріали досудового розслідування повністю чи частково фіксуються в електронному вигляді – на CD-носіях (Канада), USB флеш картах (Росія) чи планшетах (Англія та Уельс). В Китайській Народній Республіці на даний час функціонує три електронні суди в Ханчжоу, Пекіні та Гуанчжоу, які проводять інтернет засідання та оцінюють електронні докази.

В нашій державі наразі також можливе впровадження окремих аспектів електронного досудового розслідування та досвіду інших країн в цій сфері, зокрема на базі вже функціонуючого ЄРДР та з внесенням ґрунтовних змін до діючого законодавства.

Література

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р., № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 09.03.2021).

2. Патрелюк Д.А. Електронне кримінальне провадження як напрям подолання протидії кримінальному переслідуванню / *Вісник Південного регіонального центру Національної академії правових наук України* / 2018. / №15 – С. 167-176.

3. Наказ Офіса Генерального прокурора від 30.06.2020 р. №298 URL: https://zakon.rada.gov.ua/laws/show/v0298905-20#Text (дата звернення: 09.03.2021).

УДК 340.69
Тищенко Є. Ф.
кандидат юридичних наук, доцент,
Національна академія Служби безпеки України

ЩОДО АКТИВІЗАЦІЇ ДІЯЛЬНОСТІ СБ УКРАЇНИ У ВИСВІТЛЕННІ РЕЗУЛЬТАТІВ КОНТРРОЗВІДУВАЛЬНОГО ЗАХИСТУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Державна політика у різних сферах національної безпеки України спрямовується на забезпечення, серед інших, її інформаційної складової [1, ч. 4 ст. 3]. Служба безпеки України (далі СБ України, Служба) здійснює контррозвідувальний захист… інформаційної безпеки держави [1, п. 3 ч. 1 ст. 19]. Одним із варіантів демонстрації результатів такого захисту є висвітлення відомостей про успішне виконання Службою покладених на неї завдань. Така діяльність добре відома і постійно ведеться, забезпечуючи позитивний загальнопрофілактичний вплив на людську свідомість, яка є одним із об'єктів інформаційної безпеки.

Так, на офіційному сайті СБ України з'являється поточна лаконічна інформація про виявлені факти протиправних діянь, протидія яким відноситься до її компетенції, а також про відповідальність винних, що настає у підсумку. Про це ж йдеться у періодичних виступах керівників Служби або інших її уповноважених осіб. У звіті про результати роботи СБ України за дев'ять місяців 2020 р. вказано, що слідчі органів безпеки працювали по п'ятдесяти дев'яти кримінальних провадженнях за ознаками державної зради та трьох за шпигунство. Засуджено до позбавлення волі за шпигунство на 10 років громадянина КНР; за державну зраду на 12 років громадянина України, який співпрацював із ФСБ РФ; за державну зраду і диверсійну діяльність на 10 років іншого співвітчизника. Припинено достроково повноваження п'ятьох іноземних дипломатів за діяльність, яка суперечить Віденській конвенції про консульські зносини [2]. Контррозвідка провела резонансну спецоперацію із викриття високопоставленого агента ФСБ РФ, який за її завданням збирав та передавав російській стороні важливу розвідувальну інформацію. Силовиками був затриманий керівник агентурної мережі спецслужб РФ, а також учасники мережі. Зловмисники передавали інформацію, яка стосувалася військових об'єктів та воїнів АТО [3].

На телеканалах демонструються короткі сюжети про припинення Службою протиправних посягань на національну безпеку держави. Іноді з'являються передачі, в яких представлена ґрунтовніша інформація завдяки документальній, у тому числі оперативній або процесуальній фіксації, коментарям фахівців, інтерв'ю з засудженими тощо.

У Єдиному державному реєстрі судових рішень можна ознайомитися із сотнями вироків і ухвал, винесених судами за результатами розглядів кримінальних проваджень, досудове розслідування яких здійснювали слідчі органів безпеки. У цих офіційних документах обсягом від кількох до десятків сторінок містяться дещо детальніші, порівняно з наведеними вище, відомості про те, у яких формах і з застосуванням яких методів іноземні спеціальні служби проводять розвідувально-підривні акції проти України, як у деяких осіб формуються злочинні наміри, якими способами вони намагаються їх реалізувати, до яких наслідків це призвело або могло призвести, чому, у ряді випадків, винні особи розкаюються у скоєному і з'являються до органів СБ України з повинною, дійовим каяттям, добровільною відмовою від вчинення кримінальних правопорушень, хто і з урахуванням чого отримує мінімальні або максимальні строки покарання. Наприклад, обвинувальним вироком від 15 жовтня 2019 р. Крюківського районного суду міста Кременчука Полтавської області у справі № 537/4152/19 констатовано, що ОСОБА_1, будучи негативно налаштованим до чинної влади в Україні та української держави у цілому, діючи умисно, з корисливих мотивів, у період з 2 по 12 липня 2014 р., під час його перебування на відпочинку на території тимчасового окупованої АР Крим, маючи злочинний умисел, спрямований на нанесення шкоди суверенітетові, територіальній цілісності та недоторканності, обороноздатності, державній, економічній та інформаційній безпеці України, усвідомлюючи протиправність своїх дій, встановив контакт та почав конфіденційне спілкування із працівниками іноземної спеціальної служби з метою виконання завдань останніх шляхом збору та передачі протягом 2014-2019 рр., інформації щодо розвитку суспільно-політичної, соціально-економічної та військової ситуації, як в Полтавському регіоні, так і в Україні, у цілому. В судовому засіданні підсудний свою вину у вчиненні інкримінуємого йому кримінального правопорушення визнав повністю, щиро розкаявся, визнає фактичні обставини справи, суду підтвердив факт вчинення злочину за таких обставин, як це вказано в описовій частині вироку. Суд узяв до уваги ступень тяжкості та обставини злочину, їх наслідки, дані про особу обвинуваченого, його вік та стан здоров`я, відношення до вчиненого, наявність пом`якшуючих та відсутність обтяжуючих покарання обставин [4].

Однак навряд чи бажані максимально широкі верстви населення України та представників міжнародної спільноти *постійно* відстежують рух таких відомостей. Тому, на нашу думку, з метою підвищення ефективності забезпечення захисту національної безпеки держави в інформаційній сфері Службі безпеки України у названих вище та інших формах доцільно активізуватися шляхом *частішого* і *ґрунтовнішого (у доречних межах)* оприлюднення *більшої кількості* конкретних фактів про результати виконання поставлених перед нею завдань.

Література

1. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

2. Результати СБУ за 9 місяців 2020 року. URL: https://ssu.gov.ua/rezultaty-sbu-za-9-misiatsiv-2020-roku.

3. Результати СБУ за 6 місяців 2020 року. URL: https://ssu.gov.ua/novyny/7797

4. Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/Review/84912473.

УДК 342.951

Ткачук Н.А.
кандидат юридичних наук,
Апарат РНБО України

ЩОДО ПІДГОТОВКИ НОВОЇ РЕДАКЦІЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

Розробка нової Стратегії кібербезпеки України (далі – Стратегія) на сьогодні є одним із пріоритетів діяльності Національного координаційного центру кібербезпеки.

Як передбачено Законом України «Про національну безпеку України», цю роботу було розпочато за дорученням Президента України після затвердження нової Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392.

Роботу організовано в рамках діяльності міжвідомчої робочої групи, яку створено при Національному координаційному центрі кібербезпеки розпорядженням Секретаря РНБО України.

До складу робочої групи увійшли уповноважені представники основних суб'єктів національної системи кібербезпеки (а саме – СБУ, Держспецзв'язку, Національної поліції, Міноборони та Генерального штабу Збройних Сил, розвідувальних органів, Національного банку України), представники Верховної Ради України, Офісу Президента України, Секретаріату Кабінету Міністрів України, Міністерства енергетики, Міністерства інфраструктури, а також Національного інституту стратегічних досліджень, який здійснює науково-методичне забезпечення підготовки проекту Стратегії.

Стратегія кібербезпеки України (2016-2020) стала першою спробою нормативного унормування питань кібербезпеки під час активної фази гібридної агресії і сам факт її прийняття є позитивним та важливим з точки зору накопичення відповідного досвіду та створення правового підґрунтя для розбудови національної системи кібербезпеки.

Разом із тим, експертами було досягнуто одностайної думки, що однією з виявлених проблем реалізації чинної Стратегії стала надмірна широта формулювань пріоритетів та напрямів забезпечення кібербезпеки України. Більшість з них не мали зрозумілої кінцевої мети, були сформульовані як «процеси», а не «цілі», яких треба досягти, були неконкретними та абстрактними.

Під час визначення структури нової Стратегії було враховано кращі світові практики з розробки стратегій у сфері кібербезпеки. Зокрема було проаналізовано кібербезпекові стратегії Європейського Союзу, Сполучених Штатів Америки, Великої Британії, Іспанії, Норвегії та інших провідних країн.

Її положення враховують конструктивні рекомендації експертів у сфері кібербезпеки, світові тенденції у напрямі прогнозованих кіберзагроз, а також подальший розвиток нормативно-правової бази необхідної для системного і обґрунтованого підходу з вирішення нагальних проблем у сфері кібербезпеки.

Емпіричною базою для підготовки нового проєкту Стратегії стали результати низки комплексних опитувань, проведених НКЦК у взаємодії із вітчизняними науковими колами та іноземними партнерами.

Основною метою Стратегії визначено створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, а ключовими засадами, на яких ґрунтується є стримування, кіберстійкість та взаємодія.

В ході підготовки проєкту було враховано п’ятирічний досвід реалізації чинної Стратегії, для того щоб мати змогу розвивати набуті досягнення та не повторювати помилок, які завадили її реалізації в повному обсязі.

Нова Стратегія буде діяти на період 2021 – 2025 років. Координатором реалізації Стратегії визначений робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки.

Процес реалізації Стратегії буде максимально прозорим, відкритим та супроводжуватись демократичним цивільним контролем.

Фінансування заходів з реалізації Стратегії здійснюватиметься в межах видатків передбачених Державним бюджетом України для сектору безпеки і оборони, які розглядатимуться Радою національної безпеки і оборони України в порядку, визначеному Бюджетним кодексом України. Відповідно до законодавства державні органи, підприємства установи і організації, передбачатимуть у своїх планах фінансові витрати на кібербезпеку. В рамках державно-приватного партнерства, міжнародної технічної допомоги залучатимуться інвестиції, які спрямовуватимуться на розбудову національної системи кібербезпеки.

Проєктом Стратегії передбачене щорічне оприлюднення Національним координаційним центром кібербезпеки публічного звіту про стан реалізації Стратегії кібербезпеки України.

Література

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

2. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України" від 14 вересня 2020 року № 392/2020 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/392/2020#Text.

3. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" від 15 березня 2016 року № 96/2016 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/96/2016#Text.

УДК 351.861

Ткачук Н.І.
кандидат юридичних наук,
Національна академія Служби безпеки України

МЕТОДОЛОГІЧНІ АСПЕКТИ ЗАРУБІЖНОГО ДОСВІДУ ОЦІНЮВАННЯ РИЗИКІВ І ЗАГРОЗ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У багатьох розвинутих країнах розробка Стратегій національної безпеки базується на системі оцінювання ризиків і загроз. Водночас, методологія оцінювання ризиків і загроз слугує підґрунтям системи оцінювання ризиків і загроз у сфері національної безпеки. З огляду на це, дослідження методологічних аспектів зарубіжного досвіду оцінювання ризиків і загроз у сфері національної безпеки заслуговує на окрему увагу.

Оцінювання ризиків у сфері національної безпеки Великої Британії здійснюється на постійній основі за трьохетапною методологією. У найбільш загальному вигляді, на першому та другому етапах відбувається виявлення всього спектру ризиків та ранжування підтверджених ризиків за критеріями тотожності і взаємодоповнення та їх групування в категорії типових ризиків. На третьому етапі, з метою розробки типових протоколів реагування держави на надзвичайні ситуації, формується шість багатокритеріальних класів ризиків. Візуалізація оцінених ризиків здійснюється у формі табличної матриці, що побудована за двома параметрами виміру рівнів імовірності та наслідків надзвичайних ситуацій. Оцінювання зовнішніх та

внутрішніх ризиків для національних інтересів, безпеки та оборони Великої Британії в інтервалі їх прояву від п’яти до двадцяти років міститься у документі «Оцінювання ризиків у сфері національної безпеки», на основі якого розробляють Стратегію національної безпеки [1, с. 14-15]. Важливо, що такий підхід дозволяє використовувати для прогнозування ризиків імітаційне моделювання із залученням експертів та формувати бібліотеку моделей поширення ризиків, яку можна поповнювати.

Подібно до Великої Британії, система оцінювання ризиків і загроз у Королівстві Нідерландів становить базовий елемент стратегічного планування та розробки Стратегії національної безпеки. Вона передбачає щорічне оцінювання ризиків, а також сканування горизонту національної безпеки, що включає аналіз трендів і загроз національній безпеці у довгостроковій перспективі. Методологія оцінювання ризиків і загроз у Королівстві Нідерландів визначена рядом керівних настанов, зокрема, «Настановою з питань комплексного аналізу та оцінювання ризиків для національної безпеки» від 2019 р. [1, с. 19-20]. Нідерландська методологія орієнтована на моделі, які дозволяють враховувати конкретну специфіку реалізації загроз, взаємозв’язок об’єктів онтології проблематики безпеки, здійснювати прогноз, використовувати особливі знання експертів з конкретних питань, враховувати нелінійність процесів, ймовірну і неймовірну недетермінованість різних явищ і взаємозв’язків. Слід зазначити, що важливим елементом оцінювання ризиків і загроз, властивим обом країнам, є визначення типових груп загроз і їх наслідків, на основі аналізу яких розробляються універсальні протоколи узгоджених дій щодо реагування на загрози, надзвичайні та кризові ситуації на різних етапах їх реалізації.

Таким чином, аналіз методологічних аспектів зарубіжного досвіду оцінювання ризиків і загроз у сфері національної безпеки дозволяє дійти наступних висновків. По-перше, розробка й запровадження якісної єдиної методології оцінювання ризиків і загроз національній безпеці дає можливість оперативно та адекватно здійснювати порівняння та пріоритезацію загроз і їх наслідків у різних сферах на основі єдиних принципів і критеріїв. По-друге, така методологія повинна базуватися на національній культурній традиції, об’єктивних закономірностях розвитку, обґрунтовувати необхідне, а також формувати бажане, яке є адекватним можливому.

Література

1. Національні системи оцінювання ризиків і загроз: кращі світові практики, нові можливості для України: аналіт. доп. [Резнікова О.О., Войтовський К.Є. Лепіхов А.В.]; за заг. ред. О.О. Резнікової. К. : НІСД, 2020. 84 с.

УДК 342.9
Ткачук Т.Ю.
доктор юридичних наук, доцент,
Національна академія Служби безпеки України

ОНТОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Людина, володіючи здатністю розумно мислити і перетворювати світ навколо себе, створила ноосферу (від *грец. noos – розум і sphere – сфера*). Давньогрецькі філософи Платон і Аристотель вважали, що «нус» – це найбільш важлива частина людської душі: «розум»; «розумна частина душі» [1, с. 11].

У цьому антропогенному середовищі виділилися три основні сфери людської діяльності, що направляють соціальний розвиток: *виробнича, технологічна* та *інформаційна*. На сучасному етапі суспільного розвитку, завдяки своєму визначальному значенню для подальшому глобальному розвитку цивілізації, домінуючою стає інформаційна. Остання й є втіленням ноосфери про яку говорив видатний французький філософ, вчений і католицький теолог П’єр Тейяр де Шарден. Авторство даного терміну належить теж французькому мислителю, представнику католицького модернізму, математику Едуару Луі Емманюелю Жюльєн Леруа [2]. Ідеї Леруа розвинув його близький друг П’єр Тейяр де Шарден. У своїй праці «Феномен людини» П’єр Тейяр де Шарден резюмує, що найбільш проникливий дослідник нашої сучасної науки може виявити тут, що все цінне, все активне, все прогресивне, з самого початку містилося в космічному клапті, з якого вийшов наш світ, тепер сконцентровано в «короні» ноосфери [3, с. 295]. Наступним кроком розвитку людства, окрім самоконцентрації ноосфери, є приєднання її до іншого розумового центру, ступінь розвитку якого вже не потребує матеріального носія – вважав П’єр Тейяр де Шарден. Варто зазначити, що основні праці П’єр Тейяр де Шарден написав у 40-их роках минулого століття. З появою Інтернету, розвитком інформаційно-комунікаційних технологій та штучного інтелекту філософські погляди цього видатного вченого, на які Ватикан накладав заборони і вважав єретичними, сьогодні здаються цілком логічними та обґрунтованими.

За П.Т. де Шардене людство пройшло розвиток *від інстинкту до думки*. Людство дійсно навчилось мислити за декілька останніх тисячоліть, що виявилось у спадщині творів науки, мистецтва, музики, літератури, архітектури тощо і наблизилось до переходу на новий виток своєї еволюції. *Що ж буде після «думки»?* Однозначно можна стверджувати, що в основі подальших еволюційних витків людства буде покладено знання, які отримані на основі інформації, тобто її критичного аналізу. Все це може приз-

вести або до розвитку унікальних можливостей «черпати» («підключатися») до універсального глобального банку даних, або до можливостей управління колективним розумом з єдиного центру. Людський розум створив техніку наділену штучним інтелектом – розумні речі, як прийнято їх називати інтернет речі. Тепер цей породжений людиною інтелект створює для цієї людини блага, більше того він вже думає за неї. Людина створила не мов би ще один мозковий центр для себе.

У розрізі такого висновку цікавим є твердження В.І. Вернадського: «*Все людство, разом узяте, представляє нікчемну масу речовини планети. Міць його пов'язана не з його матерією, але з його мозком, з його розумом …. У геологічній історії біосфери перед людиною відкривається величезне майбутнє, якщо вона зрозуміє це і не використовуватиме свій розум і свою працю на самовинищення. Ноосфера є новим геологічним явищем на нашій планеті. У ній вперше людина стає найбільшою геологічною силою. Людина може і повинна перебудовувати своєю працею і думкою сферу свого життя, перебудовувати докорінно порівняно з тим, що було раніше. Перед нею відкриваються все ширші й ширші творчі можливості. [...] Зараз ми переживаємо нову геологічну еволюційну зміну біосфери. Ми входимо в ноосферу*» [4, с. 479].

На відміну від індустріального суспільства, яке в основі має машинну технологію, специфіка постіндустріального суспільства криється в використанні інформаційно-інтелектуальної технології. У постіндустріальному суспільстві, як зазначає відомий американський соціолог і публіцист, засновник теорії постіндустріального суспільства Д. Белл, формується нова еліта, цей прошарок суспільства реалізується завдяки компетентності і високій кваліфікації, які індивіди набувають завдяки освіті. Тепер становище в суспільстві не визначається кількістю наявної власності, що успадковується або одержується в результаті підприємництва, або певною політичною позицією, яку підтримує особистість за допомогою громадських рухів. У результаті, чільну роль теоретичного наукового знання, на думку Д. Белла, визначає положення вченого як центральної фігури в постіндустріальному суспільстві. «Постіндустріальне суспільство є суспільством знання в двоякому сенсі: по-перше, джерелом інновацій у все більшій мірі стають дослідження і розробки...; по-друге, прогрес суспільства... визначається успіхами в області знань» [5, с. 288]. Таким чином, Д. Белл визначає інформацію та знання в якості «стратегічного ресурсу» - основною силою, що породжує корінні зміни в постіндустріальному суспільстві.

Сьогодні, на наш погляд, цю ідею необхідно розглядати в якості базисної при формуванні філософської концепції інформаційної безпеки.

Література

1. Швецова-Водка Г. Учення про ноосферу як підстава розвитку ноокомунікації // Український журнал з бібліотекознавства та інформаційних наук. № 2. 2018. С. 10-22.

2. Le Roy E. Les origines humaines et Γ evolution de Γ intelligence. Paris, 1928. 376 p.
3. Тейяр де Шарден П. Феномен человека: Сб. очерков и эссе: пер. с фр. / сост. и предисл. В.Ю. Кузнецов. М.: ООО «Издательство АСТ». 2002. 553 с.
4. Вернадский В.И. Биосфера и ноосфера / Предисловие Р. К. Баландина. М.: Айрис-пресс, 2004. 576 с.
5. Белл Д. Грядущее постиндустриальное общество. М.: Academia, 1999. С. 288.

УДК УДК 004.056.18

Толюпа С.В.
доктор технічних наук, професор
Браіловський М.М.
кандидат технічних наук, доцент,
Київський національний університет імені Тараса Шевченка
Штаненко С.С.
кандидат технічних наук, доцент,
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут

ПОБУДОВА СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ МЕТОДІВ DATA MINING

Системи виявлення атак (СВА) являють собою окремий клас програмних засобів (ПЗ), під яким розуміють програми, процедури, правила, а також, якщо передбачено, супутніх їм документації та даних, що відносяться до функціонування системи обробки інформації. Використання СВА дозволяє вирішити цілий ряд завдань, що забезпечують досягнення цілей інформаційної безпеки. Технології виявлення атак постійно розвиваються й удосконалюються, і ця область постійно залучає нових виробників та розробників [1].

Метод опорних векторів (англ. Support Vector Machine, SVM) - це набір схожих алгоритмів категорії «навчання з учителем», які застосовується у задачах класифікації та регресійного аналізу. Даний метод належить до сімейства лінійних класифікаторів. Характерною особливістю методу опорних векторів є постійне скорочення емпіричної помилки класифікації і збільшення зазору між класами. Тому даний метод часто називають методом класифікатора з максимальним зазором.

Метод опорних векторів є одним з найбільш популярних методів класифікації. Метод будує оптимальну гіперплощину в просторі характеристик: $w \cdot x - b = 0$, що розділяє нормальні і аномальні елементи. У підсумку завдання можна звести до квадратичного програмування:

$$min\|w\|_H^2/2 + C\sum_{i=1}^{N}\xi_i$$

при $c_i(wx_i - b) \geq 1 - \xi_i, 1 \leq i \leq N$

де ξ_i- величина помилки на об'єктах x_i .

Метод опорних векторів має певні недоліки для застосування в задачі виявлення мережевих атак: висока залежність вирішальної функції *f(x)* від встановлюваного заздалегідь параметра C; висока чутливість до наявності шумів і викидів; потреба в масштабуванні тренувальних даних; відсутність можливості ранжувати важливість атак [3].

Метод знаходить елементи, що знаходяться на кордонах між двома класами, які і називаються опорними векторами. Метод опорних векторів здійснює пошук лінійної функції, яка дозволяє віднести елементи набору даних до одного з двох класів. Завдання бінарної класифікації може бути сформульована як пошук лінійної функції *f(x)*, яка приймає значення менше нуля для елементів одного класу й більше нуля для елементів іншого.

Розподілена гіперплощина має наступний вигляд:

$$f(x) = w * x - b = 0$$

де *w* - вектор, перпендикулярний до розподіленої гіперплощини, параметр b визначає відстань гіперплощини від початку координат.

Гіперплощина, паралельні оптимальні гіперплощини та найближчі до опорним векторах двох класів, можуть бути описані наступними рівняннями:

$$\begin{cases} wx - b = 1 \\ wx - b = -1 \end{cases}$$

Якщо навчальна множина даних лінійно нероздільні, то можна вибрати гіперплощини так, щоб в смугу між ними не потрапляла жодна точка навчальної вибірки й потім максимізувати відстань між гіперплощинами. Ширина смуги в цьому випадку дорівнює $\frac{2}{\|w\|}$, тому слід мінімізувати $\|w\|$. Для виключення всіх точок з смуги, повинна виконуватися умова: $c_i(wx_i - b) \geq 1{,}1 \leq i \leq n$, де c_i - мітка класу, що приймає значення -1 і +1, x_i - вектор робочої вибірки з міткою класу c_i . Це завдання квадратичної оптимізації еквівалентна задачі пошуку сідлової точки функції Лагранжа:

$$\begin{cases} -L(\lambda) = \sum_{i=1}^{n} \lambda_i + \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \lambda_j c_i c_j (x_i x_j) \rightarrow min_\lambda \\ \lambda_i \geq 0{,}1 \leq i \leq n \\ \sum_{i=1}^{n} \lambda_i c_i = 0 \end{cases}$$

де *L* - функція Лагранжа, λ_i - множники Лагранжа.

Щоб узагальнити *SVM* на випадок лінійної нероздільності, вводиться константа *C* - внутрішній параметр методу, що дозволяє регулювати відношення між максимізацією ширини розділової смуги й мінімізацією сумарної помилки.

Основною проблемою застосування методу опорних векторів в завданні бінарної класифікації є складність пошуку лінії кордону між двома

класами. У разі якщо такий кордон побудувати не вдається, одне з рішень - це збільшення розмірності (перенесення даних в інший простір, більш високої розмірності), де існує можливість побудови площини, що розділяє безліч елементів на два класи.

Проведене імітаційне моделювання та застосування інтелектуальної системи підтвердило правильність вибору множини методів інтелектуального аналізу даних в якості побудови систем виявлення вторгнень. Так метод опорних векторів дозволив ідентифікувати більшість атак з результатом 96-98%.

Проведені експерименти з програмним прототипом показали високу якість виявлення мережевих атак і довели правильність вибору комбінаторіки методів інтелектуального аналізу даних і застосовність вироблених методик.

Література

1. Toliupa S., Nakonechnyi V., Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system. Information technology and security. Ukrainian research papers collection Volume 7, Issue 1 (12). 2018. - с. 69-79.

2. Довбешко С.В., Толюпа С.В., Шестак Я.В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. Науково-технічний журнал "Сучасний захист інформації".– №1. 2019. С. 56-62.

УДК 004.056.53

Федорієнко В. А.
Центр воєнно-стратегічних досліджень
Національного університету оборони України
імені Івана Черняховського

ОСОБЛИВОСТІ УПРАВЛІННЯ КІБЕР-РИЗИКАМИ ПРИ ПОБУДОВІ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ

Розуміння необхідності об'єднання усіх існуючих інформаційних систем Міністерства оборони (МО) України та Збройних Сил (ЗС) України у цілісну взаємозв'язану *інформаційну інфраструктуру* [1] призвело до прийняття рішення про створення єдиної системи управління оборонними ресурсами DRMIS (Defense Resources Management Information System) та автоматизованої системи оперативного (бойового) управління C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). Створення систем DRMIS та C4ISR ґрунтується на засадах викладених у [1; 2].

Взаємодія суб'єктів доступу і об'єктів захисту повинна здійснюватися відповідно до правил кібербезпеки. Виконання таких заходів знижує ймовірність появи кібер-ризиків. Тому, питання управління кібернетичними ризиками при побудові інформаційної інфраструктури Міністерства оборони України є актуальною задачею.

Метою є визначити підходи для управління кібер-ризиками при побудові інформаційної інфраструктури Міністерства оборони України.

Сучасна тенденція визначення процесів кібербезпеки заснована на принципі нульової довіри (англ. ZeroTrust). Ідея полягає в тому, що інформаційні ресурси організації вже можуть бути скомпрометовані або будуть скомпрометовані з великою вірогідністю.

Частина загальної системи управління, яка ґрунтується на підході, що враховує ризики інформаційної безпеки такі, як "бізнес-ризики", призначені для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки, що отримала назву – система управління інформаційною безпекою, СУІБ (англ. Information Security Management System, ISMS) [3].

СУІБ мають виконувати дві задачі з точки зору кіберзахисту – фіксувати аномальну активність всередині корпоративної мережі (включаючи "хмари") та підвищити вартість атаки для кіберзлочинців (включаючи "інсайдерів"). Управління кібер-ризиками – це зниження ймовірності використання вразливостей, які можуть завдати шкоди цінним активам організації.

Процес управління кібер-ризиками включає

1. Організаційну складову – створення та забезпечення постійної роботи комітету з ризик-менеджменту.

2. Проведення ідентифікації всіх ресурсів (активів), які впливають на працездатність організації і категоризація з критичності (за методологією Factor Analysis of Information Risk, FAIR [4]): матеріальні активи (програмне і апаратне забезпечення); закрита інформація, у тому числі, конфіденційна інформація; бізнес-процеси; дані користувачів; інтелектуальна власність; репутація організації; взаємовідносини з регуляторами (compliance).

3. Визначення величини збитку при атаці на актив. Основні категорії втрат (методологія FAIR): фінансові прямі; репутаційні; здоров'я і життя

4. Визначення джерел атаки: віддалені (чорні хакери, звільнені співробітники з незакритим доступом; зовнішні (підрядники); внутрішні; вплив людського фактору (цілеспрямовані, ненавмисні); технічні збої.

5. Визначення ймовірності атаки. Для обчислення величини ризику використовують величини збитку (величини, розрахованої за методологією FAIR) та визначену ймовірність настання інциденту (проведення атаки).

6. Визначення метрик і обчислення величини кожного ризику. Для обчислення величини ризику всім зацікавленим сторонам необхідно використовувати метрики обчислення за якісними чи кількісними показниками. У

таких метриках зазначаються одиниці величин, що виражають збиток, і на якому відрізку часу.

7. Визначення заходів з управління кожним ризиком. Для прийняття рішення яких заходів необхідно застосовувати до кожного ризику необхідно порахувати економічну складову кожного варіанту.

8. Періодичний перегляд та моніторинг ризиків.

Таким чином побудова кібербезпеки інформаційної інфраструктури Міністерства оборони України повинна включати процеси управління кібер-ризиками.

Література

1. Закон України Про захист інформації в інформаційно-телекомунікаційних системах: Закон від 05.07.1994 № 81/94-ВР / [Електронний ресурс] // Верховна Рада України – Режим доступу: http://zakon5.rada.gov.ua/laws/show/80/94- вр/ed20111231

2. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року “Про Стратегічний оборонний бюлетень України” [Електронний ресурс]: указ [видано Президентом України 06 червня 2016 р. №240/2016]. – Режим доступу:http://www.president.gov.ua/documents/ 2402016-20137.

3. Аналіз нормативно-правових та організаційно- технічних аспектів забезпечення інформаційної безпеки / [В. В. Овсянніков, С. В. Дехтяр, С. А. Паламарчук та ін.]. // Сучасні інформаційнітехнології у сфері безпеки та оборони. – 2015. – №3. – С. 187–192.

4. Modeling modern network attacks and countermeasures using attack graphs / [K. Miller, M. Chu, R. Lippmann та ін.]. // Annual Computer Security Applications Conference. – 2009. – С. 117–126.

УДК 659.4:327.88.

Фурашев В.М.
кандидат технічних наук,
старший науковий співробітник,
НДІ інформатики і права НАПрН України

ДО ПРІОРИТЕТНИХ НАПРЯМІВ РОЗВИТКУ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПЕРІОД ДО 2030 РОКУ

Говорити про те, що в Україні відсутня система інформаційної безпеки, особливо з точки зору нормативно-правового забезпечення, не зовсім вірно. За 30 років незалежності в Україні вже створена досить повна нормативно-правова база забезпечення інформаційної безпеки людини, суспільства і держави, яка відповідала минулим та, багато у чому, або значною частиною, і сучасним викликам і загрозам в інформаційній сфері.

На наш погляд, подальший розвиток системи інформаційної безпеки, зокрема її нормативно-правової складової, та її ефективності, зокрема що

стосується ступеня підвищення швидкості та адекватності реагування щодо запобігання і усунення новітніх реальних та потенційних загроз в інформаційній сфері, буде значною мірою залежати від:

- впорядкованості нормативно-правової бази забезпечення інформаційної безпеки, у першу чергу, законодавчої;
- ступеня реальності правозастосовної діяльності в інформаційній сфері;
- наявності, рівню професіоналізму та насиченості фахівцями, спроможними аналізувати та класифікувати, відповідно до положень чинного законодавства та інших нормативно-правових актів, процеси та події, які відбуваються або поширюються в інформаційному просторі. у тому числі і контентну складову.

Цілком природно, що наведені фактори, які впливають на розвиток системи інформаційної безпеки, не є вичерпними, але, на наш погляд, саме ці фактори, на даний час, є визначальними.

Процеси, процедури та дії у сфері забезпечення інформаційної безпеки здійснюються на основі відповідної нормативно-правової бази, у першу чергу - законодавчої, в інформаційній сфері. Інформаційне законодавство формувалося поступово у часі, при чому досить не системно; під різні погляди, цілі, мету; як реагування на об`єктивні та суб`єктивні потреби та ін. Це не могло не призвести до елементів дублювання, неоднозначності трактувань тих чи інших положень, понятійно-категорійних тлумачень та багато-багато іншого. Питання щодо необхідності впорядкування законодавчої бази в інформаційній сфері, починаючи з 1992 року, неодноразово піднімалося на самих високих рівнях всіх гілок влади, але й донині не зрушило з місця.

Головними принципами щодо *впорядкування інформаційного законодавства*, на наш погляд, мають бути:

- усунення дублювання. Законодавче визначена загальна класифікація інформації по ступеню доступу до неї, правила поводження з інформацією (обробка, поширення, збереження та знищення) повинні бути єдиними та сконцентрованими в одному «місці», незалежно від сфери застосування. Не може бути 20-ти видів таємної інформації. Таємна інформація є таємною і правила поводження з нею мають бути однаковими. Специфічні, галузеві вимоги до правил поводження з інформацією, за необхідності, вирішуються галузевими нормативно-правовими актами, які погоджуються з Міністерством юстиції України. Не повинно бути у законах України двох і більше визначень одного і того ж терміну, за виключенням об`єктивної необхідності та наукової обґрунтованості;
- усунення неоднозначності тлумачення положення/положень (за сукупністю) законів України в інформаційній сфері;

- усунення «камуфляжних» термінів та їх визначень, які фактично описуються у відповідних положеннях Закону;

- усунення положень, які не впливають на регуляторну функцію процесу/суспільних відносин.

Процеси забезпечення безпеки, апріорі, пов`язані з процесами визначеного обмеження об`єкта захисту у здійсненні визначених процесів та процедур життєдіяльності. Конституція України, закони України «Про інформацію», «Про друковані засоби масової інформації (пресу) в Україні» та інші встановлюють досить повний та чіткий перелік спрямованості інформації, яку заборонено поширювати будь-якими засобами та попереджають щодо юридичної відповідальності за ці правопорушення. Також слід підкреслити, що правила поводження з інформацією не залежать від виду простору (природному – інформаційному або штучному – кібернетичному) у якому вона циркулює, форми її представлення та її носіїв.

Але, на практиці, ми спостерігаємо діаметрально протилежну ситуація, яка свідчить про практичну відсутність *реальної правозастосовної діяльності в інформаційній сфері.* Прикладів на користь даного твердження – безліч. Кожен з нас щоденно з цим стикається, причому правопорушення у зазначеній сфері здійснюються, починаючи з самих «верхів» до самих «низів». Необхідно чітко розуміти, що *реальної* правозастосовної діяльності та всіх її складових *системи* інформаційної безпеки в Україні не буде, незважаючи на будь-які наміри. Саме правозастосовна діяльність, спираючись на впорядковане інформаційне законодавство, надасть системності та комплексності системі інформаційної безпеки України, зробить її ефективною.

Необхідно чітко розуміти, що питання впорядкованості законодавчої бази забезпечення інформаційної безпеки, з точки зору наявності висококваліфікованих фахівців, для України не є проблемним. Вирішення даного питання залежить лише від бажання, у першу чергу політичного, та часу, а також фінансування. Інша проблема, яку необхідно вирішувати, це проблема налагодження та забезпечення функціонування правозастосовної діяльності в інформаційній сфері. Без наявності та необхідної насиченості більшості сфер забезпечення життєдіяльності суспільства кваліфікованими фахівцями, спроможними аналізувати та класифікувати процеси та події, які відбуваються або поширюються в інформаційному просторі, у тому числі і контентну складову, відповідно до чинного законодавства та інших нормативно-правових актів, дану проблему не вирішити.

В цьому напрямку в Україні багато чого вже зроблено, але ще більше - попереду.

УДК [001.8/.816/.817] + 001.92 +004.031.42+007.2
Хлапонін Ю.І.
доктор технічних наук,
Київський національний університет будівництва і архітектури
Козубцова Л.М.
кандидат технічних наук
Козубцов І.М.
кандидат технічних наук, професор РАЕ,
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут

ПРО ОДИН З ПРІОРИТЕТНИХ НАПРЯМКІВ НАУКОВО-ОБҐРУНТОВАНОГО СУПРОВОДЖЕННЯ РОЗВИТКУ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Національна безпека держави є одним з основних факторів стабільного розвитку суспільства. Проте Збройні сили України (ЗС) зіткнулися з веденням гібридної війни проти себе із застосуванням кіберпростору, а це вимагає перегляду існуючих підходів до гарантування та підтримки національної безпеки України. Сучасні війська потребують постійного оновлення озброєння і військової техніки. Для своєчасного врахування та прогнозування сучасного стану озброєнь в ЗС України постала необхідність у суб'єктах наукової і науково-технічної діяльності (НіНТД), а саме: наукові і науково-педагогічні працівники, ад'юнкти і докторанти та інші вчені Збройних сил, які створюють наукову (науково-технічну) продукцію в інтересах оборони держави.

Висвітлити один з пріоритетних напрямків науково-обґрунтованого супроводження розвитку забезпечення кібернетична безпека.

В контексті опису "Майбутнє безпекове середовище 2030. Аналіз стратегічного передбачення" виконаного дослідниками Військового інституту телекомунікацій та інформатизації за окремим дорученням Директора Департаменту воєнної політики, стратегічного планування та міжнародного співробітництва Міністерства оборони України окреслено, що до 2030 р. і надалі зберігатиметься негативна тенденція до руйнування системи освіти і науки в Україні через зниження видатків на їх фінансування, втрату науково-виробничої бази України, виникнення колізій у системі законодавства як результат необґрунтованих, з наукової точки зору, рішень щодо вибору вектору реформування вищої освіти та науки України [1].

Сьогоднішня реальність підтверджує думку С.К. Булгакова та А.І. Субетто, що результатом реформ є лише зміна загальної канви на державному рівні, а ось далі, на технологічному рівні, все відбувається на стереотип-

ному застарілому фундаменті, що не відповідає сучасним глобальним викликам культурологічної парадигми [2, с. 224 – 240].

Зазначені фактори призводять до збільшення розриву культури між старшим поколінням дослідників, достатньо мотивованим і налаштованим на подальшу роботу у військовій системі НіНТД, та новим поколінням, яке має іншу природу мотивації і схильне до відтоку з цієї системи. Це спричинено значною мірою відносно низьким рівнем заробітної плати. Тенденція і досі продовжується, трансформуються лише її форми та причини (академічна мобільність, необхідність публікуватися у наукових періодичних виданнях інших держав, SciVerse, Scopus, Web of Science), що є передумовою витоку з України наукових результатів, технологій та інших важливих перспектив, які охоплюють державний і військовий сектор. Таким чином відбувається «добровільна передача» державної таємниці службам науково-технічної розвідки іноземних держав, які є власниками цих наукометричних баз та окремих видань [3-5].

За даними Державної служби статистики України, кількість випускників ВВНЗ, що виявляють бажання стати суб'єктами НіНТД у НУ, складала 1% від загальної чисельності. Їх адаптація в колективі неможлива без застосування «діалогу культур» та системи військових традицій. Зважаючи на всі обставини, ми вважаємо, що методологічна культура ад'юнктів не дістала належного висвітлення в наукових дослідженнях з підготовки фахівців інформаційної та кібернетичної безпеки [6]. І це означає, що її необхідно підняти на новий рівень.

Висновки. Отже, на даний час є нагальною потребою вирішенні наступних завдань: 1) розвитку методологічної культури ад'юнктів з напрямку підготовки інформаційна безпека; 2) призупинення норми обов'язкового опублікування у наукових періодичних виданнях інших держав (Scopus, Web of Science), оскільки це ключова умова витоку з України наукових результатів у сфері захисту інформації та кібербезпеки, технологій та інших важливих перспектив, які охоплюють державний і військовий сектор; 3) рекомендувати створити і вести роз'яснювальну роботу про створення аналогічної наукометричної бази України на базі бібліотеки ім. В.І. Вернадського.

Література

1. Ващенко А.Н., Козубцов И.Н. Направления развития института аспирантуры системы третьего уровня высшего образования в контексте Болонской хартии // Бизнес. Образование. Право. Вестник Волгоградского института бизнеса. 2013. №3 (24). С. 68 – 71.

2. Булдаков С.К., Субетто А.И. Философия и методология образования: Научное издание. Кострома: Изд-во КГУ им. Н.А. Некрасова, 2002. 444 с.

3. Козубцов И.Н. О влиянии научных индексов цитирования на Национальную безопасность и стратегию развития государства в современной научной картине мира знаний // Гілея: науковий вісник. Збірник наукових праць. 2013. Випуск 74(№7). С.230 – 232.

4. Козубцов И.Н. О междисциплинарной связи мотива к научной публикации с инвестиционным показателем // Поколение будущего: Взгляд молодых ученых – 2013:

материалы Международной молодежной научной конференции (13-15 ноября 2013). Курск: Юго-Западный государственный ун-т, 2013. Т.2. С. 189 - 193.

5. Козубцов І.М., Куцаєв В.В. Філософія інформаційної безпеки в умовах її кібернетичного розповсюдження в сучасної динамічній наукової картині світу на прикладі надання знань молодим вченим та студентам // Гілея: науковий вісник. Збірник наукових праць. 2013. Випуск 73(№6). С. 291 – 293.

6. Хлапонін Ю.І., Козубцов І.М., Хлапонін Д.Ю., Рябчун Ю.В. Науково-педагогічний компетентнісний моніторинг підготовки фахівців в галузі інформаційної безпеки // Державно-управлінські студії №4(6), 2018. http://studio.ipk.edu.ua/naukovo-pedahohichnyy-kompetentnisnyy-monitorynh-pidhotovky-fakhivtsiv-v-haluzi-informatsiynoyi-bezpeky.

УДК 343.34:352.07

Черниш Р.Ф.
кандидат юридичних наук, доцент,
Національна академія Служби безпеки України

ЄДИНИЙ ІНФОРМАЦІЙНИЙ ПРОСТІР СИСТЕМИ БЕЗПЕКИ ГРОМАД: ПОЗИТИВНІ ТА НЕГАТИВНІ АСПЕКТИ ФУНКЦІОНУВАННЯ

На території України (мм. Київ, Дніпро, Харків, Житомир тощо) реалізуються цільові програми «Безпечне місто», в процесі яких створюється міська система відеоспостереження - єдиний інформаційний простір безпеки громад.

«Безпечне місто» - це сукупність IP-периферійного та базового відео- і комп'ютерного обладнання, кабельних мереж, мережевого та комунікаційного обладнання, пристроїв гарантованого безперебійного електроживлення та спеціального програмного забезпечення, що дозволяє автоматизувати процес ведення відеоспостереження в цілодобовому режимі за окремими ділянками території міста, зберігати та обробляти отриману інформацію [2].

Впровадження системи он-лайн відеоспостереження дало певні позитивні результати: в її рамках створено відповідні ситуаційні центри міст, за її допомогою співробітниками правоохоронних органів розкриваються злочини та правопорушення, забезпечується оперативне реагування на аварійні ситуації тощо.

Водночас, у процесі аналізу інформації щодо дієвості вказаної системи виявлено низку загроз національній безпеці держави, що може призвести до негативних наслідків.

Зокрема, в мережі Інтернет на офіційних ресурсах органів державної влади та місцевого самоврядування переважно відсутній повний перелік

встановлених камер із зазначенням їх місць розташування та місць, нагляд за якими здійснюється.

Також, відсутня єдина система обліку камер відеонагляду, що дозволяє зацікавленим стороннім особам самостійно їх встановлювати, прикриваючись реалізацією міської програми, при цьому використовувати встановлені камери для здійснення злочинної діяльності проти громадської безпеки (підготовка терористичних актів, шпигунство, крадіжки, посягання на особисте життя міських мешканців тощо).

Також, до загроз державній безпеці у вказаній сфері необхідно віднести загальнодоступність значної кількості встановлених камер в мережі Інтернет. На даний час доступ до встановлених міською радою та приватними суб'єктами відеокамер можливо здійснити з будь-якого ПЕОМ, маючи лише підключення до мережі Інтернет. У свою чергу, моніторинг користувачів мережі Інтернет, що здійснюють доступ до зазначених сервісів, не здійснюється жодним державним органом чи установою.

На нашу думку, вказана загальнодоступність та відсутність контролю може призвести до нанесення суттєвої шкоди інтересам держави, адже здійснюючи моніторинг відеонагляду за державними установами та організаціями можливо зібрати інформацію щодо співробітників, відвідувачів організацій, наявності працівників на робочому місці, розпорядок дня та іншу особисту чи компрометуючу інформацію щодо громадян України [3].

Враховуючи сучасний розвиток технологій, в процесі якого на вулицях міст заявились сотні відеокамер, на даний момент в державі відсутній Закон, відповідно до якого повинен здійснюватись контроль за встановленням та здійсненням відеонагляду, чинними нормами не передбачено правоохоронного чи контролюючого органу, що здійснює контроль у даній сфері.

Беручи до уваги стрімкі темпи діджиталізації багатьох сфер країни (у т.ч. сфери громадської безпеки), розвиток Інтернет-злочинності та нестабільну зовнішньополітичну ситуацію навколо України виникає необхідність реальної та своєчасної ліквідації окресленого ряду загроз, що можуть бути використані на шкоду інтересам країни [1].

Систематизуючи викладене, з метою забезпечення державної безпеки України, усунення недоліків чинного законодавства, збереження особистого та приватного життя громадян країни, а також попередження злочинності, вважається за доцільне на рівні Верховної ради України прийняти нормативний акт, яким:

- зобов'язати суб'єктів, що здійснюють встановлення та користування відеонаглядом, здійснювати реєстрацію розташування камер та серверів у відповідних органах місцевого самоврядування;
- для органів місцевого самоврядування передбачити обов'язок реєстрації місць розташування камер відеонагляду, серверів, на які здійснюється

запис отриманої інформації, та осіб, що здійснили встановлення приладів та їх власників;

- встановити відповідальність за несанкціоноване встановлення та використання відеонагляду;
- визначити компетенцію щодо контролю у сфері відеонагляду за відповідним правоохоронним органом.

Література

1. Roman Chernysh, Viktoriya L. Pogrebnaya, Iryna I. Montrin, Tetiana V. Koval and Olha S. Paramonova. Development of Internet communication and social networking in modern conditions: institutional and legal aspects. *Revista San Gregorio* (special issues Nov). Url: http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/.

2. Антон Геращенко: Інтеграція приватних відеокамер спостереження до системи «Безпечне місто» зробить країну безпечнішою. URL: https://www.kmu.gov.ua/news/anton-gerashchenko-integraciya-privatnih-videokamer-sposterezhennya-do-sistemi-bezpechne-misto-zrobit-krayinu-bezpechnishoyu.

3. Черниш Р.Ф. Соціальні мережі, як один із інструментів накопичення та протиправного використання персональних даних громадян. *Проблеми законності*. 2017. Вип. 136. С. 205-214.

УДК 305 : 355.01

Чеховська М.М.
доктор економічних наук, професор
Гребенюк В.М.
доктор юридичних наук, старший дослідник,
Національна академія Служби безпеки України

ГЕНДЕРНІ АСПЕКТИ ГІБРИДНОЇ ВІЙНИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ

Еволюція форм та методів ведення гібридної війни зумовлює необхідність напрацювання симетричних та асиметричних засобів протидії. Одним із елементів гібридної війни Російської Федерації є намагання дискредитувати курс нашої держави на європейську та євроатлантичну інтеграцію, зокрема шляхом нівелювання основних демократичних цінностей сучасного суспільства, до яких відноситься просування політики рівних прав і можливостей жінок і чоловіків, або гендерної політики. Застосовуючи інформаційно-психологічний, релігійний та політичний вплив, відбувається активне намагання кардинально змінити смислове та змістовне навантаження сутності гендерної політики з прогресивного на регресивне.

У сучасній Росії саме гібридна війна розглядається як основний спосіб військових дій. Підтвердженням цьому є російські наукові розробки у га-

лузі ведення гібридних війн, наявність у росіян (М. Хамзатов, Ю. Балуєвський, А. Манойло, В. Багдасарян) чітких систематизованих знань з цієї проблеми.

Російськими фахівцями визнається, що комплекс зусиль, які прикладаються у гібридній війні, конвергенція методів війни зарекомендували себе як дієвий спосіб здобуття переваги над противником та його ослаблення навіть за обмежених людських та матеріальних ресурсів. Наголосимо, що стратегія гібридної війни має наступні складові: суто військову (класичну), військово-політичну, економічну та інформаційну. Всюди для перемоги важливим є комплекс цих зусиль.

У своїх доробках щодо типології війн майбутнього російський журналіст, воєнний експерт І. Попов розглядає асиметричний конфлікт, як один із проявів гібридної війни, скрізь призму гендерної моделі, в якій аналізується нерівність сторін у фізичному та матеріальному аспектах [7]. Так, покладаючись на концепцію, викладену Є. Месснером щодо відповідності психіки регулярного війська чоловічій психіці, і, відповідно, відповідності психіки іррегулярного ополчення – жіночій психіці [5, с. 60], І. Попов надає авторські рекомендації щодо розв'язання асиметричного конфлікту. Зокрема, він пропонує не лише «підвищувати психологічну культуру командирів і штабів регулярних збройних сил, а й більш активно залучати до планування бойових дій проти іррегулярних формувань військових спеціалістів-жінок» [6].

Гібридна війна Російської Федерації проти України набула соціального виміру. Мова йде про маніпуляцію гендерними питаннями в контексті ведення Російською Федерацією політики з дискредитації євроінтеграційного та євроатлантичного курсу Української держави. Саме на зазначеному аспекті наголошує Ю. Лапутіна, вказуючи на використанні соціальних та гендерних стереотипів у маніпуляціях поняттям гендерної рівності, як сучасного тренду когнітивної війни Російської Федерації проти України [2].

Так, в Україні набула поширення інформаційна кампанія, «яка полягає в нагнітанні надуманих «страхів» та залякування суспільства нібито «загрозливою гендерною ідеологією», що підтримується різними організаціями, які отримали назву антигендерних рухів, що мають суттєвий вплив на суспільну свідомість» [3].

У своїй публікації Є. Магда, досліджуючи гендерні виклики гібридної війни, наголошує на таких аспектах, як інформаційно-психологічний вплив на жіночу аудиторію та використання жіночого образу для отримання необхідного пропагандистського або деструктивного ефекту [4, с. 132-133]. Так, у першому випадку мова йде про застосування інформаційних атак з метою створення жіночого протестного руху (влітку 2014 року матері та дружини військовослужбовців протестували проти проведення ротації вій-

ськових та проти мобілізації тощо), або руху підтримки (цькування та образи полонених військовослужбовців, зокрема в окупованому Донецьку, а також участь жінок в іррегулярних незаконних збройних формуваннях та окупаційній адміністрації Російської Федерації). У другому випадку інформаційні ресурси використовують фейкові сюжети, в яких жінка або дівчина є, зокрема, об'єктом нападу (історія січня 2016 року про російськомовну дівчинку Лізу у Німеччині), або наче є свідком ганебних та жорстоких дій (розповідь жінки у липні 2014 року про розп'ятого на її очах хлопчика).

Підсумовуючи зазначимо, що серед напрямів державної політики щодо забезпечення рівних прав та можливостей жінок і чоловіків є спрямованість на «захист суспільства від інформації, спрямованої на дискримінацію за ознакою статі» [1]. На сьогоднішній день поширення вказаної інформації є одним із компонентів розгорнутої Російською Федерацією кампанії проти політики гендерної рівності, що реалізується в Україні. Своєчасне визначення гендерних гібридних загроз дозволить вчасно їх нейтралізувати або зменшити негативний, зокрема інформаційний, вплив на громадян, суспільство та державу в цілому.

Таким чином, гендерні гібридні загрози – це явища, тенденції та чинники, що створюються штучно з використанням різнорідних засобів та методів (політичних, економічних, соціальних, інформаційних, психологічних, національних, релігійних, етнічних) введення в оману або нейтралізації заходів із впровадження політики гендерної рівності з метою створення дилем та отримання диспропорційних результатів [8, с. 178].

У сучасних умовах соціально-політичних трансформацій ми пропонуємо наступну класифікацію гендерних гібридних загроз: за локалізацією загрози – внутрішні, зовнішні, регіональні та глобальні; за сферами впливу – політичні, соціальні, інформаційні, освітні, культурні, історичні та інші; за характером – фальсифіковані, маніпулятивні, пропагандистські; за об'єктами – спрямування на громадян, суспільство, державні та недержавні органи, державу; за суб'єктами, або джерелами загроз – державного, недержавного, національного, іноземного походження; за спрямуванням – точкові, або спрямованої дії, та комплексні; за джерелом виникнення – регіональні, терористичні.

Література

1. Закон України від 8.09.2005 року № 2866-IV «Про забезпечення рівних прав та можливостей жінок і чоловіків». URL : https://zakon.rada.gov.ua/laws/show/2866-15 (дата звернення: 22.06.2020).

2. Лапутіна Ю.А. Маніпуляція поняттям гендерної рівності – поточний тренд когнітивної війни. Інформаційна безпека людини, суспільства, держави. 2019. № 2 (26). С. 125-134.

3. Левченко К.Б. Інструменти здійснення маніпуляцій навколо змісту та напрямів державної гендерної політики. Інформаційна безпека людини, суспільства, держави. 2019. № 2 (26). С. 135-143.

4. Магда Є. Жінка як ціль та інструмент у гібридній війні. European Political and Law Discourse. 2017. Volume 4. Issue 3. P. 131-136.

5. Месснер Е.Э. Всемирная мятежвойна. М. : Directmedia, 2013. 508 с.

6. Попов И. Ассиметричный конфликт: гендерная модель. URL : http:// uturewarfare.narod.ru/research.html?clk23985023612921937731 43=1. (дата звернення 22.06.2020).

7. Попов И.М., Хамзатов И.М. Война будущего: Концептуальные основы и практические выводы. Очерки стратегической мысли. М. : Кучково поле, 2016. 832 с.

8. Чеховська М.М. Гібридні загрози у забезпеченні гендерної рівності в Україні. Актуальні проблеми впливу збройного конфлікту на Сході України на появу й поширення гендерно обумовленого насильства та забезпечення доступу до правосуддя: зб. тез наук. доп. наук.-практ. конф. (Київ, 18 верес. 2020 р.). Упоряд.: М.Г. Вербенський, В.О. Рядінська, Ю.Б. Ірха, О.І. Бочек. Київ : ДНДІ МВС України, 2020. С. 175-179.

УДК 355.40

Шарий О.В.
кандидат політичних наук,
Військова частина А1906

РОЗВІДУВАЛЬНІ ОРГАНИ УКРАЇНИ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІНОЇ БЕЗПЕКИ ДЕРЖАВИ

Стрімкий розвиток інформаційних технологій, активне застосування методів гібридної війни проти нашої держави, зміни в законодавстві України, що сталися останніми роками, вимагають перегляду ролі та місця розвідувальних органів держави в забезпеченні її національної безпеки, насамперед її інформаційної складової.

Відповідно до Концепції розвитку сектору безпеки і оборони України [1] розвідувальні органи України (РОУ) є невід'ємною складовою сектору безпеки і оборони України. На них покладаються виконання таких основних завдань: своєчасне забезпечення споживачів розвідувальною інформацією, сприяння реалізації національних інтересів України, протидія зовнішнім загрозам національній безпеці України у визначених законом сферах [2]. При цьому однією з основних функцій РОУ є виявлення та визначення ступеня зовнішніх загроз національній безпеці України, у тому числі у кіберпросторі.

Відповідно до нового Закону України «Про розвідку» оновлено розподіл сфер діяльності РОУ: Служба зовнішньої розвідки України здійснює розвідувальну діяльність у зовнішньополітичній, економічній, військово-технічній, науково-технічній, інформаційній, екологічній сферах, сфері кібербезпеки; водночас розвідувальний орган Міністерства оборони України

здійснює розвідувальну діяльність у воєнній сфері, сферах оборони, військового будівництва, військово-технічній та кібербезпеки.

З метою виконання покладених завдань у визначених сферах розвідувальної діяльності РОУ мають створити/реформувати структурні підрозділи, відповідальні за виконання завдань із забезпечення кібербезпеки.

у доповіді проаналізовані основні фактори, які істотно ускладнюють та негативно впливають на розвідувальну діяльність у сфері кібербезпеки. Основними такими факторами є:

технологічні досягнення, що допомагають об'єктам розвідки краще приховувати та берегти свої секрети;

зусилля розвідки мають охоплювати все більші території й щоразу більшу кількість діючих суб'єктів, тому суттєво ускладнюються планування, управління, збір і аналіз, які потребують дедалі більшої гнучкості;

збільшується кількість несподіваних ситуацій, які виникають у непередбачуваній комбінації неконвенціональних загроз. Щоб запобігти цьому, РОУ мають створювати широку мережу джерел інформації, які потрібно моніторити лише для того, щоб бути постійно обізнаним стосовно ситуації;

співробітники розвідки мають володіти багатьма мовами спілкування. Для цього потрібно витрачати значні ресурси на обробку матеріалів та їх переклад;

значне збільшення масивів інформації, мереж та засобів комунікації, з одного боку, спрощує можливість доступу до них, а з другого, створює проблему вибору;

втрата монополії і державного контролю над криптологією, вільний доступ до технології наскрізного шифрування інформації, оптико-волоконні системи передачі тощо ускладнюють можливості з перехоплення та оперативного дешифрування;

застосування нових типів цифрового радіозв'язку (стільникового, супутникового), що мають зашифровані канали передачі інформації, зменшує кількість доступних джерел інформації;

збільшення кількості споживачів розвідки та їхніх потреб;

скорочення часу на виявлення та реагування на загрози;

необхідність постійно бути в тренді новітніх технологій передачі, зберігання, шифрування інформації потребує значних ресурсів на наукові дослідження та розробку новітніх засобів розвідки;

недостатньо конкурентний рівень оплати праці співробітників розвідки порівняно з аналогічною роботою у сфері кібербезпеки на цивільному ринку праці.

Цей перелік не є вичерпним. Вищеокреслене накладає значні обмеження на обсяг завдань у сфері кібербезпеки, що можуть бути виконані розвідувальними органами, та потребує дуже ретельного планування розподілу сил і засобів за завданнями, створення нових розвідувальних можливостей у межах існуючого ресурсу.

Подальші наукові дослідження слід спрямувати на розробку нових способів та методів виявлення загроз у сфері кібербезпеки, запобігання їх виявлення та протидії їм.

Література

1. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року “Про Концепцію розвитку сектору безпеки і оборони України” : Указ Президента України від 14.03.2016 р. № 92/2016. URL: http://www.president.gov.ua/documents/922016-19832 (дата звернення: 20.02.2021).

2. Про розвідку : Закон України від 17.09.2020 р. № 912-IX. URL: http://zakon.rada.gov.ua/laws/show/912-20#Text (дата звернення: 20.02.2021).

УДК 658.004.343

Шевченко О.А.
кандидат юридичних наук,
Національна академія Служби безпеки України

ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА – ПРІОРИТЕТНІ НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

Необхідною умовою успішного розвитку України як прогресивної, правової, демократичної держави є входження її до міжнародного співтовариства. Але це тягне за собою і появу певних соціально-економічних, політичних та юридичних проблем. Однією з них є зростання економічної злочинності із новими видами кримінально караних діянь, особливо таких, як злочини інформаційної спрямованості. Особливої небезпеки набуває зрощування злочинів у сфері інформаційної безпеки з таким кримінально караним діянням як легалізація (відмиванням) доходів, одержаних злочинним шляхом, що досить негативно впливає на сталий розвиток нашої держави та ставить системні перепони на шляху інтеграції до Євросоюзу та Північно-Атлантичного альянсу.

Саме тому, у ст. 3 Рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України" чітко наголошено Кабінетові Міністрів України, державним органам за відповідними сферами національної безпеки подати у шестимісячний строк на розгляд Ради національної безпеки і оборони України проекти відповідних стратегій і програм безпекової сфери, в тому числі, Стратегію економічної безпеки, Стратегію інформаційної безпеки, Стратегію кібербезпеки України [1].

В той же час, нова Стратегія національної безпеки України «Безпека людини – безпека країни», що затверджена указом Президента України №392/2020 14 вересня 2020 року у ст. 9 розділу ІІ, який регламентує поточні

та прогнозовані загрози національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов, чітко наголошує, що стрімкі технологічні зміни, насамперед в енергетиці та біотехнологіях, розробки у сфері штучного інтелекту тощо докорінно трансформують економіку і суспільство в цілому. Стрімко зростає роль інформаційних технологій у всіх сферах суспільного життя. Розробляються системи озброєнь на основі нових фізичних принципів, із використанням квантових, інформаційних, космічних, гіперзвукових, біотехнологій, а також технологій у сфері штучного інтелекту, створення нових матеріалів, робототехніки та автономних безпілотних апаратів [2].

Таким чином, фіксуємо виважену, своєчасну і визначальну роль вищих інститутів влади і управляння держави, а саме, Президента України, Ради національної безпеки і оборони України та Кабінету міністрів України у впорядкуванні актуальних проблем управління інформаційною безпекою держави з чітким посиланням в цьому контексті на необхідність забезпечення економічної безпеки України.

Література

1. Рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України" [Електронний ресурс] // сайт Верховної Ради України. – Режим доступу:https://zakon.rada.gov.ua/laws/show/n0005525-20#n2

2. Стратегія національної безпеки України «Безпека людини – безпека країни», що затверджена указом Президента України №392/2020 14 вересня 2020 року [Електронний ресурс] // сайт Президента України. – Режим доступу: https://www.president.gov.ua/documents/3922020-35037.

УДК 355.451

Шидлюх В.В.
Руснак С.О.
Національний університет оборони України
імені Івана Черняховського

ВЗАЄМОДІЯ ЯК ЕЛЕМЕНТ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ

Налагодження продуктивних стратегічних комунікацій є безсумнівним пріоритетом розвитку інформаційної і національної безпеки України.

За прийнятими в НАТО підходами, взаємодія органів військового управління, особливо вищих керівників з місцевими органами влади, громадськими діячами, лідерами суспільної думки та іншими стейкхолдерами в районі операцій, є складовою стратегічних комунікацій і може зробити зна-

чний внесок у формування сприятливого середовища, досягнення необхідних ефектів та мети місії, особливо якщо ці завдання ретельно плануються, грамотно виконуються та працюють на перспективу.

Успішна взаємодія у значній мірі залежить від завчасного планування, зорієнтованості на ефектах, цілеспрямованості, інтегрованості і координованості, повноти використання можливостей особистого спілкування, проактивності, перспективності заходів, а також створеної мережі взаємодії.

Завчасне планування має важливе значення для максимізації ефективності кожного виду діяльності. Замисел взаємодії має бути частиною загальної стратегії та плану взаємодії. Перспективи взаємодії повинні бути довгостроковими та довготерміновими.

Успішні заходи взаємодії мають мати на меті прив'язаність до стратегічного наративу місії та цілей. В ідеалі з вимірюваними результатами. У більшості ситуацій взаємодія пов'язана з обміном повідомленнями, що витікають із замислу стратегічних комунікацій, що забезпечують цілеспрямоване інформування стейкхолдерів, задля досягнення необхідних ефектів.

Особи (ключові лідери, особи, що безпосередньо беруть участь у реалізації стратегії взаємодії, зокрема, особи, що приймають рішення), а також необхідний персонал, мають бути ретельно підібрані на основі їх здібностей, впливовості, доступності та взаємосумісності.

Взаємодія повинна здійснюватися як цілісна функція, що включає врахування різних напрямків роботи. Дуже важливо, щоб усі зацікавлені підрозділи включали свої інформаційні вимоги до взаємодії в процесі планування заходів, а також існувала система зворотного зв'язку (інформування) для розуміння зацікавленими сторонами поточного стану та вчасного корегування цих заходів.

Взаємодія повинна проводитись один на один (особисто), хоч і не обов'язково очно. В ідеальній ситуації особисте спілкування використовується для посилення передачі та інтерпретації повідомлень. Взаємодія може відбуватися і телефоном, через соціальні медіа чи електронною поштою, але в такому разі зміст і форма повідомлення повинні бути такими, щоб учасник відчував, ніби з ним розмовляють особисто. Незалежно від того, яким чином ведеться спілкування, взаємодія повинна зміцнювати та рухати вперед взаємні стосунки, сприяти довірі та співпраці.

Планувальники взаємодії повинно передбачати розвиток можливостей, так би мовити дивитись за межі обрію і передбачати відкриття нових можливостей для залучення потенційно зацікавлених осіб. На додаток до регулярних офіційних зустрічей, візитів, стратегічні заходи можуть бути сплановані на фоні конференцій, навчань, інформувань, спільних культурних заходів тощо, тобто практично в кожній принагідній ситуації.

Результат взаємодії відображається на результатах діяльності як усього угруповання, так і окремого штабу, а також посадової особи, яка проводить

взаємодію. З цією метою важливо, щоб усі заходи взаємодії були синхронізовані щодо тем, контенту зустрічей (спілкування) та відгуків про події. Всі ці заходи мають бути узгодженими та взаємопідтримуючими. Створення мережі взаємодії має важливе значення для цього процесу. Оскільки діяльність із взаємодії є такою ж важливою частиною повсякденної діяльності військ, як і виконання бойових завдань, ця мережа повинна існувати як у мирний час, в кризу, так і в особливий період для забезпечення повної підтримки військ.

Для реалізації ефективної програми взаємодії необхідно розробляти: стратегію, план та матрицю взаємодії.

Стратегія взаємодії встановлює довгострокову мету взаємодії.

План взаємодії надає більш докладну інформацію про те, як саме повинна бути реалізована стратегія.

Матриця взаємодії надає включає інформацію про те, коли саме мають відбутися заходи взаємодії, а також історичні записи про те, що і коли вже відбулося раніше.

Функція стратегічних комунікацій в операціях полягає у досягненні за допомогою особистого спілкування, спілкування за допомогою засобів масової інформації та соціальних медіа когнітивного ефекту, який багатократно підвищує ефективність операції.

Взаємодія, як елемент стратегічних комунікацій, це не просто план, а продуманий, збалансований та ефективний когнітивний продукт, який впроваджується в інформаційний простір через тісну співпрацю військових та невійськових суб'єктів комунікації і забезпечує всебічну підтримку і забезпечення виконання конституційних завдань Збройними Силами України.

Література

1. PO (2009) 0141, NATO Strategic Communications Policy. NATO. – 2009.
2. MC 0628, NATO Military Policy on Strategic Communication. NATO. – 2017.
3. NU 0692, NATO StratCom Handbook. NATO. – 2017.
4. NU 0706, NATO Engagement Handbook. NATO. – 2017.

УДК 341

Шлапаченко В.М.
кандидат юридичних наук,
старший науковий співробітник,
Національна Академія Служби безпеки України

РОЗВІДУВАЛЬНА ТАЄМНИЦЯ: ПРОБЛЕМНІ ПИТАННЯ ЗАПРОВАДЖЕННЯ НОВОГО ВИДУ ТАЄМНОЇ ІНФОРМАЦІЇ

З прийняттям у вересні 2020 р. Закону України «Про розвідку» в правовому полі держави з'явилося нове поняття – розвідувальна таємниця

(далі – РТ). Цей закон (п. 6 ст. 1) визначає її як «вид таємної інформації, що охоплює відомості та дані, отримані або створені розвідувальними органами України під час виконання покладених на ці органи завдань та здійснення функцій, визначених цим Законом, розголошення яких може завдати шкоди функціонуванню розвідки і доступ до яких обмежено відповідно до цього Закону в інтересах національної безпеки України».

При цьому законодавець не встановлює чіткого розмежування двох різновидів таємної інформації, - державної та розвідувальної, а лише зазначає (ч. 2 ст. 46) що «інформація про розвідувальну діяльність, про методи розвідки, сили і засоби розвідки, розвідувальна інформація, інформація про забезпечення споживачів розвідувальною інформацією, про взаємодію розвідувальних органів з іншими суб'єктами розвідувального співтовариства, з державними органами, органами місцевого самоврядування, підприємствами, установами, організаціями, компетентними органами іноземних держав, міжнародними організаціями належить до таємної інформації та підлягає віднесенню у встановленому законом порядку до розвідувальної таємниці та/або державної таємниці».

Відповідно до ч. 4 ст. 46 вимоги до віднесення, організації та забезпечення режиму поводження з інформацією, що належить до РТ, визначаються Президентом України, у тому числі на основі пропозицій координаційного органу з питань розвідки.

Також, в Законі «Про розвідку» (ч. 5 ст. 46) зазначається, що «забезпечення безпеки інформації, що належить до РТ, від несанкціонованих дій (випадкових чи навмисних), що призводять, зокрема, до її витоку, зміни, блокування або втрати, здійснюється розвідувальними органами у визначеному ними порядку. Відповідальність за незаконну передачу або збирання, розголошення, зміну, блокування, знищення інформації, що належить до розвідувальної таємниці, встановлюється законом».

До сьогодні переліку відомостей, що становлять РТ (на кшталт ЗВДТ) до загального відома не опубліковано, жодної відповідальності за її втрату, незаконні розголошення чи передачу іноземним адресатам законодавством не встановлено.

Без сумніву, що відомості, віднесені до РТ, становитимуть інтерес для спецслужб іноземних держав і виступатимуть об'єктом їх розвідувальних спрямувань. Втім, відповідь на питання чи будуть ці відомості об'єктом контррозвідувального захисту на сьогодні не виглядає такою ж однозначною, оскільки протидія розвідспрямуванням щодо РТ в рамках КРС ускладнюється відсутністю правового механізму визначення цього виду таємної інформації, як предмета суспільно-небезпечного і протиправного посягання та, відповідно, кримінальної відповідальності за його можливі форми (розголошення, втрату, передачу (збирання з метою передачі) іноземцям тощо),

а також статусу цих правопорушень як тяжких чи особливо тяжких злочинів, який би дозволив для запобігання їм застосовувати контррозвідувальні та оперативно-розшукові заходи, пов'язані з тимчасовим обмеженням прав та законних інтересів особи (ч. 3 ст. 8 Закону «Про ОРД»).

Крім того, наділення розвідувальних органів правом проведення контррозвідувальних заходів з метою забезпечення власної безпеки (ч. 2 ст. 17 Закону «Про розвідку») та одночасне зобов'язання СБ України здійснювати контррозвідувальне забезпечення Збройних Сил України та інших військових формувань, до яких належать і розвідувальні органи (ст. 24 Закону «Про СБУ») породжує певну неврегульовану конкуренцію суб'єктів КРД.

З аналізу наведених законодавчих положень вбачається, що за своєю сутністю РТ є дуже близькою до службової інформації у сфері РД. При цьому варто зауважити очевидну законодавчу прогалину, - відсутність згадки про таку інформацію у п. 2 ч. 1 ст. 9 Закону України «Про доступ до публічної інформації» (визначається, яка інформація може належати до службової). Відтак, вважаємо за необхідне доповнити зазначений пункт терміном «розвідувальна діяльність» і викласти його у такій редакції: «зібрана в процесі оперативно-розшукової, контррозвідувальної, *розвідувальної* діяльності та у сфері оборони країни, яку не віднесено до державної таємниці», застосувавши ці зміни і до ст. 330 КК України, де ця інформація визначається предметом злочину.

Крім того, доводиться констатувати, що цей законодавчий прецедент створює передумови запровадження (за аналогією) інших видів таємної інформації у сферах державної діяльності, наприклад: контррозвідувальної таємниці, поліцейської таємниці, військової таємниці, прикордонної таємниця, податкової таємниці політичної таємниці тощо. За умов збереження в законодавстві інститутів державної таємниці (з диференційованими грифами секретності) та службової інформації, а також з огляду на заплановану реформу цих інститутів за стандартами НАТО, такі новації, на наш погляд, не сприятимуть покращенню охорони та контррозвідувального захисту державної інформації з обмеженим доступом.

Вважаємо, що віднесення інформації, що визначена РТ, до державної таємниці з грифом «Таємно» чи до службової інформації з грифом «Для службового користування» (з запропонованими вище змінами до ст. 9 Закону «Про доступ до публічної інформації», та, відповідно, до ст. 330 КК) усунуло б (а точніше, – і не створювало б) зазначені проблеми та тенденції до їх збільшення через ймовірність запровадження інших видів таємної інформації у сферах державної діяльності.

УДК 140.8
Штоквиш О.А.
кандидат філософських наук,
старший науковий співробітник,
Національна академія Служби безпеки України

МАНІПУЛЮВАННЯ ІСТОРИЧНОЮ СВІДОМІСТЮ ЯК СКЛАДОВА ГІБРИДНОЇ ВІЙНИ

Ні для кого не є секретом, що на сьогодні саме розвиток інформаційної сфери характеризує розвиток суспільства. Сучасне суспільство вже не може нормально функціонувати без застосування інформаційних систем, без забезпечення надійності їх функціонування, вдосконалення процесів обробки інформації, захисту від протиправного доступу до неї. Така залежність суспільства та особистості від інформації, яка стала свого роду соціальним ресурсом, робить суспільну та індивідуальну свідомість дуже вразливою до дій спрямованих на її дезорганізацію та руйнування. Подібні тенденції активно впливають на стан політичної, економічної, воєнної безпеки держави. Сформувалась дуже важлива залежність національної безпеки від забезпечення безпеки інформаційної, яка буде постійно зростати відповідно до розвитку інформаційної сфери та інформаційних технологій.

У воєнній сфері зазначені тенденції призвели до докорінних змін у характері і способах ведення війн. Не захоплення території, розгром ворожої армії, а нав'язування своєї ідеї – ось що гарантує перемогу у сучасному світі. Причому особливого значення набувають ідеї пов'язані з тим сегментом свідомості спільнот, який прийнято називати колективною або історичною пам'яттю. Здобути перемогу у такій інформаційно-психологічній війні означає зруйнувати значущість світу історичних ідей у якому спільнота зберігає маркери власної ідентифікації із яким позиціонує свою присутність у світі. Саме тому чільне місце у подібних війнах надається маніпулюванням історичною свідомістю.

Як показав досвід російсько-української війни на Донбасі, досить ефективними виявилися методи впливу на історичну свідомість певної соціальної (національної, етнічної, регіональної) групи з метою коригування, переформатування або знищення її колективної пам'яті, оскільки, пам'ять завжди пов'язана з існуванням певної ідентичності (національної чи іншої) і, по суті, є фундаментом, несучою конструкцією, на якій тримається остання.

Росія веде проти України гібридну війну надаючи особливого значення застосуванню різноманітних методів з арсеналу інформаційно-психологічної війни, намагаючись не просто вплинути на загальний морально-бойовий стан українських збройних сил, а й деморалізувати найширші верстви

населення, а, за можливості, зруйнувати саму національну ідентичність українців. Саме тому чільне місце в її інформаційних атаках надається маніпулюванням історичною свідомістю, особливо пов'язаним з темою пам'яті Другої світової війни. Така пріоритетність обумовлена наявністю у значної частини населення колишнього СРСР специфічного світосприйняття, яке обумовлено функціонуванням у суспільній свідомості т.зв. міфу Великої Перемоги.

Даний міф, як і будь-який інший сучасний політичний міф, за змістом є політично маркованою, акцентованою та адаптованою для сприйняття широким загалом інформацією, яка не потребує перевірки та аргументації; за функцією є засобом маніпулятивного корегування суспільної свідомості та інструментом у боротьбі за завоювання, легітимізацію та втримання влади. В основі міфу лежать архетипічні праобрази добра, зла, героя, спасителя; архетипічні сюжети боротьби, кінця світу, спасіння. Відповідно до сучасного їх наповнення, формується модель світосприйняття, яка, з допомогою різних специфічних прийомів транслюється, а, по суті, навязується суспільству.

Одним із таких прийомів є спеціальне використання мовних засобів для внесення коректив у мовну картину світу даної спільноти, з метою прив'язки понять, термінів, мовних штампів, смислових кліше до явищ, подій, ідей, з якими вони раніше не мали безпосереднього зв'язку. Це здійснюється умисно з метою внести бажані зміни у суспільну свідомість шляхом створення віртуальної політичної реальності. Матеріалом для створення нової мовної реальності слугує реальна жива мова спільноти, яку піддають спеціальній обробці, внаслідок чого вона стає придатною для нав'язування, за допомогою слів, лексики певної політичної позиції суспільству. Подібна практика вдало змальована (хоч і у жанрі політичної сатири) геніальним англійським письменником Джорджем Оруеллом у його безсмертному романі «1984». Йдеться про так званий «новояз» – тобто «мову тоталітарного суспільства.

Так, створюючи на основі застосування асоціативних лексико-семантичних елементів повязаних з поняттям «фашизм» певні смислові одиниці («укронацисти», «каратели», «хунта», «гауляйтери» тощо), пропагандистського кшталту, путінські фахівці інформаційно-психологічної війни намагаються «обробляти» ними свідомість як населення самої РФ так і України.

Фундаментальні дослідження витоків і генези тоталітаризму дають підстави вважати, що створення методик дискурсивного управління суспільством шляхом спеціального використання мовних засобів притаманне усім тоталітарним режимам, оскільки, пов'язане з самою природою тоталітарного управління. Також важливо враховувати, що результатом подібного маніпулятивного впливу є утворення свідомості тоталітарного типу, що здатна легко продукувати та сприймати міфи. Основною характеристикою

даної свідомості є статичне мислення, відповідно до законів якого, процес оцінювання реалій об'єктивної дійсності відбувається не шляхом критичного раціонального міркування, а за допомогою заздалегідь сформованих у свідомості розумових стереотипів, що призводить до руйнації у людини автономії волі та здатності до незалежного мислення та врешті до деградації особистості.

УДК 004.056

Шуклін Г.В.
кандидат технічних наук,
Державний університет телекомунікацій

ПРОБЛЕМА МОДЕЛЮВАННЯ КЕРУВАННЯМ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ В УМОВАХ ІНФОРМАЦІЙНОЇ ЕКСПАНСІЇ

Життя в сучасному світі неможливо уявити без інформації. Розвиток інформаційних технологій, які на теперішній час пов'язані з інтернетом, об'єднало всіх людей в єдиний інформаційний простір. Відкритий доступ до інформації, яку можна аналізувати, дало можливість її переробляти, розширювати та створювати нову для подальшого розповсюдження. Це призводить до можливостей впливати на підсвідомість особи, групи осіб, громадян держави та цілих народів. Одним із механізмів таких дій є інформаційна експансія. Саме цей інструментарій є основою для того, щоб для окремої групи людей всі інші здійснювали свої вчинки відповідно певним сценаріям, які формуються та розповсюджуються через відповідні інформаційні джерела. На теперішній час не існує чіткого однозначного поняття словосполученню «інформаційна експансія», однак це поняття постійно використовується в різних інформаційних джерелах.

Поняття експансії є многозначним, однак з перекладу з латинської «expansio» це слово означає – розповсюдження. Спираючись на В. Ліпкана, «інформаційна експансія» - це цілеспрямоване вкидання інформації, яка спрямована на зміну у заданому ракурсі сприйняття відповідної події для обраної цільової аудиторії [1]. Український експерт, полковник запасу В'ячеслав Гусаров терміну «інформаційна експансія» дав наступне визначення: комплекс заходів, який направлено на захоплення інформаційних каналів з метою впливу на думку населення і формувати інші думки та змісти у відповідної групи населення [2]. Дані визначення дають можливість стверджувати, що інформаційна експансія – це не що інше, як спосіб лобіювання. В енциклопедичному довіднику В.Б. Вепринцева, інформаційна експансія визначається, як придбання та встановлення сфер впливу в інформа-

ційному просторі з використанням для цього сукупного інформаційного потенціалу та засобів силового інформаційного впровадження [1]. Інформаційну експансію за своїм змістом, можна розкласти на дві складові, які породжують інформаційно-психологічну експансію (рис.1).

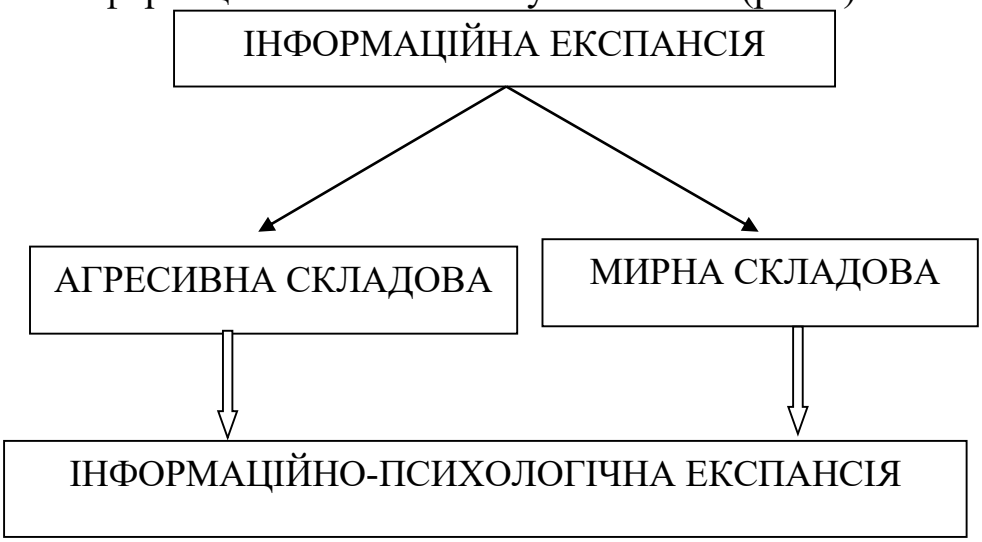


Рис. 1. Складові інформаційної експансії

Агресивна складова інформаційної експансії – це досягнення інформаційного впливу для геополітичного домінування над опонентами шляхом інформаційної війни, яка відбувається без використання військової зброї. Використовуючи інформаційну війну, як засіб військової політики, дає можливість не створювати пряме військове вторгнення в держави, які стали мішенями такої агресії, та залишати мирні відносини з ними, незважаючи на збитки, які ці держави понесли. Ці збитки навіть можуть бути більшими, якщо б на території цих держав були традиційні бойові дії.

Мирна складова інформаційної експансії – має два прояви, які можна назвати інформаційно-психологічним, та науково-технічним.

Інформаційно-психологічний прояв – це впровадження у свідомість як індивідуальну так і масову наукової, культурної та політичної еліти і населення країни, яка є об’єктом експансії, моральних цінностей, для зміни в цій державі системи соціальних відношень в тому напрямку, який потрібен для інформаційно-психологічної залежності від країни, з боку якої відбувається експансія. Зміна соціальних відношень в суспільстві відбувається завдяки пропаганді та розповсюдженню культурних досягнень в літературі, музиці, театрі, кіно, продукції ЗМІ, релігійного прозелітизма, ініціатив створення та підтримки певних політичних партій та громадських організацій.

Науково-технічний прояв – це створення умов технічної та технологічної залежності науки та економіки держави, яка є об’єктом експансії, від сучасних науково-технічних розробок та продуктів інформаційних технологій країн, до яких застосовується інформаційна експансія.

Застосовуючи дві складові, які були охарактеризовані вище, інформаційна експансія породжує інформаційно-психологічну експансію метою якої є непомітну для суспільства повільну зміну системи соціальних відносин, яка необхідна країні, яка є джерелом експансії. Завдяки інформаційно-психологічній експансії здійснюється витиснення положень національної ідеології і національної системи цінностей, та заміна їх власними. Це призводить до впливу і своєї присутності в державі, яка є донором, та встановленні контролю над стратегічними ресурсами, інформаційно-телекомунікаційною структурою та національними ЗМІ.

Література

1. Вепринцев В.Б. Операции информационно – психологической войны: краткий энциклопедический словарь - справочник / В.Б. Вепринцев, А.В. Манойло, А.И. Петренко, Д.Б. Фролов; под ред. А.И. Петренко – 2-е изд., стереотип. – М.: Горячая линия – Телеком, 2011. – 495 с.

2. Гухман В.Б. Информационная экспансия / В.Б. Гухман // Актуальні проблеми міжнародних відносин. Випуск *ІІІ (Частина І)*, 2012. – с. 21-28.

УДК 351: 303.732.4 : 004.056

Якименко Ю.М.
кандидат військових наук,
Державний університет телекомунікацій

МЕТОДИЧНІ ПІДХОДИ СИСТЕМНОГО АНАЛІЗУ ДО ВИРІШЕННЯ ПРОБЛЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Реальність сьогодення, яке складається у світі, вимагає принципово нових підходів до осмислення ситуацій, що складаються. Особливо це важливо для України як і усіх інших країн, які переживають етап кардинальних трансформаційних, а сьогодні – і кризових змін, відродження державності. Оскільки держава являє собою складну систему, то забезпечення її стабільності можна розглядати з використанням методології дослідження складних систем і з позицій системного аналізу. При аналізі проблем функціонування складних систем з наукових інструментів системного аналізу зазвичай використовують методи: сценаріїв, діагностичний, дерева цілей, економічного аналізу, експертних оцінок. [1] Ситуація з поширенням коронавірусної хвороби (СОУЮ-19) виявила низьку готовність багатьох країн світу до реагування на загрозу масштабної пандемії, засвідчила недосконалість національних систем їх кризового менеджменту, а також наявність суттєвих уразливостей безпеці їх економічній, соціальній, інформаційній діяль-

ності. На перший план виходять питання вдосконалення системи національної безпеки країни, зокрема визначення ефективних механізмів комплексного реагування на загрози на всіх етапах їх виникнення, підвищення готовності держави і суспільства в цілому шляхом запровадження універсальних методичних підходів та практичних дій по координації такої діяльності.

У зв'язку з поширенням пандемії коронавірусу Україна зіштовхнулася з проблемними питаннями управління, пов'язаними в першу чергу з загрозами її системи національної безпеки, які треба вирішувати:

• неможливість раннього виявлення, оцінювання і попередження загроз;

• відсутність достатніх можливостей, резервів, альтернативних стратегій на випадок відповідної кризової ситуації, що загрожує національній безпеці;

• відсутність або неактуальність планів комплексного реагування на загрози, єдиних стандартів та узгоджених протоколів дій (зокрема, щодо запровадження обмежувальних заходів в умовах карантину), на державному, регіональному та місцевому рівнях;

• недосконаліть системи стратегічного планування й аналізу загроз в державі, у тому числі стосовно проведення комплексного оцінювання впливу загрози та відповідних заходів реагування на різні сфери національної безпеки, моніторингу ефективності заходів реагування тощо.

• повільне реагування на загрозу з боку уповноважених державних і місцевих органів антикризового управління, низька ефективність координації заходів на різних рівнях, у т. ч. через недоліки законодавства та/або його невиконання. [2]

У багатьох країнах світу існуючі національні системи оцінювання загроз і пов'язаних з ними ризиків дозволяють виявляти небезпечні тенденції та загрози для національної безпеки, а також уразливості в державі та суспільстві. За результатами дослідження кращих світових практик з методології управління оцінюванням загроз і ризиків у різних країнах світу можна виділити основні етапи управлінської діяльності:

1. Визначення найбільших загроз для національної безпеки у сферах економічної, соціальної, суспільно-політичної, екологічної тощо за визначеними критеріями (індикаторами) у динаміці.

2. Поглиблений аналіз можливих наслідків загроз, розробка сценарних прогнозів кожної загрози, моделювання і виявлених найбільших загроз.

3. Оцінка можливостей, виявлення уразливостей, забезпечення безперервності критично важливих функцій держави.

4. Можливі сценарії розвитку кризових ситуацій та їхні наслідки, поширення результатів оцінювання ризиків (національні реєстри ризиків у відкритому доступі на офіційних урядових сайтах), комплексний звіт про виявлені загрози.

5. Моніторинг і повторне оцінювання загроз і ризиків з урахуванням отриманого досвіду.

Беручи до уваги те, що забезпечення національної безпеки – це один із пріоритетів державної політики України на сучасному етапі, актуальним питанням є створення національної системи оцінювання ризиків і загроз як підсистеми в системі забезпечення національної безпеки держави. Як самостійна система, вона має стати ефективним інструментом прийняття рішень у сфері національної безпеки та кризового управління, важливим елементом стратегічного планування, сприятиме підвищенню рівня готовності держави та суспільства до реагування на широкий спектр загроз. Вона не повинна обмежуватися лише оцінками ризиків і загроз, а обов'язково має охоплювати оцінювання можливостей, необхідних для ефективного реагування на загрози на різних етапах розгортання кризової ситуації.

Таким чином, національна система оцінювання ризиків і загроз в Україні має охоплювати такі процеси: оцінювання та ранжування ризиків і їх наслідків; розроблення сценарних прогнозів; оцінювання відповідних можливостей; виявлення уразливостей; візуалізація та поширення отриманих результатів; моніторинг та перегляд оцінок ризиків.

Література

1. Якименко Ю. М. Системний аналіз методологічних підходів до управління підприємством у сфері інформаційних технологій. // II Міжнародна науково-практична конференції «Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку», 11лютого 2021 року.— Київ: ДУТ, 2021. - С. 279-282. URL: http://www.dut.edu.ua/uploads/n_9074_59003267.pdf.

2. Исследование систем управления.Учебно-методический комплекс по дисциплине.- Липецк: 2015-178с. URL: https://rucont.ru/file.ashx?guid=5246af5b-a443-4b99-a30f-34575f6f3f2e.

ОРГАНІЗАЦІЙНО-ПРАВОВІ ПРОБЛЕМИ ЗАХИСТУ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

УДК 004.738.5

Ахрамович В.М.
кандидат технічних наук, доцент,
старший науковий співробітник,
Державний університет телекомунікацій

РОЗРОБКА МЕТОДУ РОЗРАХУНКУ ЗАХИСТУ ІНФОРМАЦІЇ ВІД РЕПУТАЦІЇ КОРИСТУВАЧІВ ПРИ НЕЛІНІЙНІЙ ЗАЛЕЖНОСТІ ПАРАМЕТРІВ

Системи довіри і репутації можуть забезпечити захист користувача від таких загроз, більш того вони можуть захистити саму систему (так звані надійні системи, Trusted systems).

Вихідна система рівнянь:

$$\begin{cases} \dfrac{dI}{dt} = \alpha Z + \beta_1 I - \sum\limits_{k=2}^{\infty} L_k I_0^k \sin^k \omega t, \\ \dfrac{dZ}{dt} = \beta_2 I + \gamma - \sum\limits_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} \quad (1)$$

де: I – потік інформації, Z - показник захисту, $\sum\limits_{k=2}^{\infty} L_k I_0^k \sin^k \omega t$ - нелінійність системи захисту Z_p – коефіцієнт, що відображає вплив заходів щодо захисту інформації; Cv – коефіцієнт, що відображає вплив швидкості витоку інформації; C_k – коефіцієнт, що відображає вплив кількості інформації на їх витік. де C_{d2} – коефіцієнт, що відображає вплив розмірів системи на захищеність; C_{d1} – коефіцієнт, що відображає вплив захищеності на витік інформації. $\gamma = (R_{d1} + R_{d2})$ – коефіцієнт, що відображає вплив репутації.

Рівняння математичної моделі з урахуванням (1), після рішення відносно коефіцієнту захисту інформації та репутації. прийме вигляд (2).

Проведемо моделювання процесу захисту інформації від коефіцієнтів репутації користувачів. Моделювання цього процесу проводиться за моделлю вираз (2), яка описує залежність захисту інформації від репутації. Графік залежності захисту інформації від репутації користувачів представлено на рис. 1.

$$Z(t)=\int[-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)-\beta_1(R_{d1}+R_{d2})+\beta_1\sum_{k=2}^{\infty}K_kZ_0^k\sin^k\omega t]\times$$

$$[\left(-C_{d2}-C_{d1}\right)\times\sum_{k=2}^{\infty}L_kI_0^k\sin^k\omega t]\times \tag{2}$$

$$\times\left((1-e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\frac{e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}})-(1-e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\frac{e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}}\right)dt$$

Аналіз графіка рис.1 показує, що зі зростанням коефіцієнтів репутації захист інформації зростає, але тільки до коефіцієнта кількості інформації 0,57. Тобто це рівень коли кількість інформації залежить від коефіцієнта репутації, практично, за лінійним законом. Зростання кількості інформації та зростання коефіцієнтів репутації приводять до зростання захисту інформації в соціальної мережі. Після досягнення коефіцієнта кількості інформації 0,57. Це є точка максимального об'єму інформації яку може захистити система захисту інформації в залежності від коефіцієнта репутації. Подальше зростання коефіцієнту репутації не приводить до підвищення захисту інформації у соціальної мережі, що відповідає дійсності та доводить вірогідність отриманих результатів.

Рис. 1. Графік залежності захисту інформації від репутації користувачів

С метою визначення стійкості системи визначимо фазовий портрет системи захисту інформації, при зовнішніх впливах на систему захисту із урахуванням коефіцієнтів репутації.

За основу будемо брати рівняння

$$\frac{d^2Z}{dt^2}-\beta_1\frac{dZ}{dt}-\alpha\beta_2Z=-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)-\beta_1(R_{d1}+R_{d2})+ \tag{3}$$

$$+\beta_1\sum_{k=2}^{\infty}K_kZ_0^k\sin^k\omega t-\beta_2\sum_{k=2}^{\infty}L_kI_0^k\sin^k\omega t$$

Рішення проведемо в програмі MatLab/Multisim методом натурного моделювання. З цією метою побудуємуу схему згідно рівняння (3) у програмному середовище Multisim.

Графік фазового портрету системи захисту інформації від коефіцієнтів репутації.

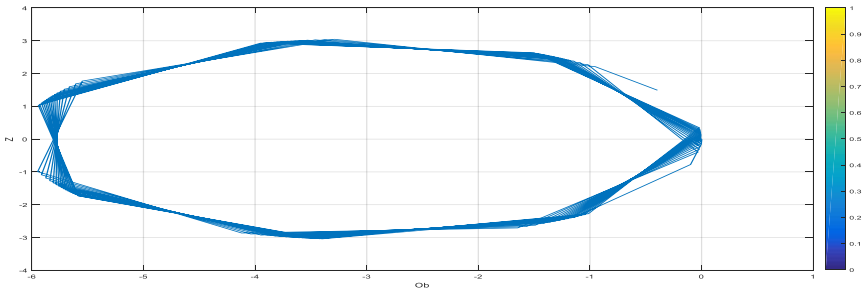


Рис. 2. Фазовий портрет системи захисту при мах значенні впливів та, репутації - 1, всі інші параметри системи захисту – 0.5

Графік наведений на рис. 2, це замкнута лінія, яка має форму, що нагадує еліпс, що вказує на стійкість системи захисту інформації. Це доводить вірність запропонованої моделі та усієї теорії розробки захисту інформації від коефіцієнту репутації.

Література

1. Ахрамович В.М. Моделі довіри та репутації користувачів в соціальних мережах. Сучасний захист інформації. К. ДУТ. 2019. №4. с. 45–51.

2. Ахрамович В.М. Модель взаємовідносин користувачів в соціальних мережах. Сучасний захист інформації. К. ДУТ, 2019. № 3. С. 42 – 50.

УДК 004.056.5

Бакалинський О.О.
кандидат технічних наук
Пахольченко Д.В.
Сапожнік Т.М.
Адміністрація Державної служби спеціального зв'язку
та захисту інформації України

АНАЛІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Процес створення нормативно-правової бази у сфері захисту критичної інформаційної інфраструктури в державному масштабі розпочався з прийняттям Закону України «Про основні засади забезпечення кібербезпеки України» яким визначено, що критична інформаційна інфраструктура – це сукупність об'єктів критичної інформаційної інфраструктури. Водночас, від-

повідно до зазначеного Закону об'єкт критичної інформаційної інфраструктури характеризується як комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури.

Щодо розкриття поняття об'єкта критичної інфраструктури (далі – ОКІ), то зазначений вище Закон визначає, що критично важливі об'єкти інфраструктури (ОКІ) – це підприємства, установи та організації, діяльність яких безпосередньо пов'язана з технологічними процесами або наданням послуг, що мають велике значення для промисловості та економіки, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду або становити загрозу для життя і здоров'я людей [1].

Події останніх років в Україні та світі, а також аналіз сучасних кіберзагроз свідчать про нагальну необхідність забезпечення надійного кіберзахисту інформаційних, комунікаційних систем та систем управління технологічними процесами ОКІ, особливо таких секторів, як енергетика, інформаційні технології, хімічна промисловість та інші.

Теоретичні та практичні результати, що пов'язані із забезпеченням кіберзахисту ОКІ, викладені в значній частині публікацій вітчизняних вчених [2-4] та зарубіжних методичних рекомендаціях. Проте, незважаючи на значну кількість підходів до забезпечення кіберзахисту ОКІ, зазначена тематика залишається актуальною, перспективною та такою, що містить велику кількість не вирішених питань.

Відповідно до постанови Кабінету Міністрів України від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» (далі – постанова КМУ № 518) кіберзахист ОКІ забезпечується шляхом впровадження на об'єкті критичної інформаційної інфраструктури ОКІ комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю [5].

Варто зазначити, що вимоги постанови КМУ № 518 відповідають більшості вимог міжнародного стандарту ISO/IEC 27001:2013. Таким чином, якщо на підприємстві, яке визначено як ОКІ, побудована система управління інформаційною безпекою (далі – СУІБ) у відповідності до міжнародного стандарту ISO/IEC 27001:2013, вимоги постанови КМУ № 518 будуть виконуються у повному обсязі.

Відповідно до вимог постанови КМУ № 518, створення системи інформаційної безпеки об'єкта критичної інформаційної інфраструктури ОКІ повинно здійснюватися відповідно до вимог технічного завдання на створення системи інформаційної безпеки. Розробці такого технічного завдання передує оцінка ризиків на об'єкті критичної інформаційної інфраструктури

ОКІ. В якості методичної основи для оцінки ризиків на об'єкті критичної інформаційної інфраструктури ОКІ постанова КМУ № 518 пропонує стандарт ДСТУ ISO/IEC 27005 [5].

З огляду на зазначене можна зробити перший висновок, що кіберзахист ОКІ забезпечується шляхом створення та впровадження на його об'єкті критичної інформаційної інфраструктури системи інформаційної безпеки, впровадження якої дозволить виконати більшу частину вимог до СУІБ, що відповідає вимогам стандартів серії ISO/IEC 27000.

Варто зазначити, що СУІБ, які відповідають вимогам стандартів серії ISO/IEC 27000, на сьогодні впроваджені і успішно функціонують на деяких ОКІ України, зокрема, у фінансовому секторі, газовидобувній галузі та енергетичному комплексі. Варто зазначити, що національна банківська система у повному обсязі ввела вимогу до наявності СУІБ в будь-якій банківській установі (постанова Національного банку України від 28.09.2017 № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України»).

Щодо розробки та впровадження СУІБ на ОКІ, у роботі [3] автор зазначав, що в процесі побудови СУІБ на ОКІ, власник організації/установи/підприємства будь-якої форми власності має оцінювати і обробляти ризики інформаційної безпеки, а також, на підставі оцінки ризиків здійснювати вибір заходів щодо захисту ресурсів (тобто щодо обробляння ризику), в тому числі і державних інформаційних ресурсів, як тих, які є найбільш важливими активами організації.

Найбільш відомі і широко розповсюджені в світі методики побудови СУІБ запропоновані міжнародними або національними стандартами ISO/IEC 27001, IT-Grundschutz, BSI, NIST 800-53, а також консалтинговими компаніями.

Водночас автор відзначив, що жоден з існуючих стандартів не містить конкретних методик формування проектних вимог до СУІБ (тобто, стосовно побудови СУІБ в конкретній організації, на конкретному ОКІ).

З огляду на зазначене можна зробити другий висновок, що актуальним є завдання розроблення формальної моделі сектору (підсектору) критичної інфраструктури та змістовної моделі ОКІ визначеного сектору (підсектору) критичної інфраструктури. Дослідження параметрів таких моделей може дати розуміння того, на які аспекти кібербезпеки необхідно звертати пильну увагу та які характеристики повинні бути реалізовані при створенні СУІБ на ОКІ в залежності від особливостей сектору (підсектору) критичної інфраструктури. Відповідно, відкритим залишається питання розроблення національної методики управління ризиками на ОКІ.

Література

1. Верховна Рада України. 7 сесія. (2017, жовт. 5). Закон № 2163-VIII, Про основні засади забезпечення кібербезпеки України. [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/laws/show/2163-viii.

2. Гончар С.Ф. Методологія оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури: дис. на здобуття наукового ступеня доктора техн. наук: 05.13.21, Київ, 2020.– 326 с.

3. Бакалинський О.О. Модель та методи визначення проектних характеристик систем управління інформаційною безпекою: монографія, Київ, Україна: ТОВ «Три К», 2020, ISBN: 978-966-7690-51-9.

4. Мохор В.В., Богданов О.М., Бакалинский О.О. та Цуркан В.В., «Дескриптивний аналіз аналогій між системами управління інформаційною безпекою та масового обслуговування», Захист інформації, т. 19, № 2,с. 119-126, 2017.

5. Кабінет Міністрів України. (2019, черв. 19). Постанова № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» // [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/518-2019-%D0%BF.

УДК 004.056.5

Бондаренко І.П.
Департамент інформатизації
Міністерства внутрішніх справ України

НОРМАТИВНЕ ВРЕГУЛЮВАННЯ ПИТАНЬ СТВОРЕННЯ СИСТЕМ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ ДЕРЖАВИ, АНАЛІЗ ТА ПРОПОЗИЦІЇ

На сьогодні нормативне врегулювання питань забезпечення інформаційної та кібербезпеки держави знаходиться на початковому етапі. Відсутній системний підхід до вирішення цих питань, зокрема і у нормативному врегулюванні. В більшості випадків інформаційна безпека зводиться до захисту інформації.

В останні роки все більше уваги приділяється питанням забезпечення кіберзахисту, зокрема, об’єктів критичної інфраструктури.

Законодавство у сфері захисту інформації розвивалося і удосконалювалося з початку незалежності України.

У 1994 році Верховною Радою України прийнято Закон України «Про захист інформації в автоматизованих системах», який трансформувався у Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

Державним комітетом України з питань державних секретів та технічного захисту інформації, а в подальшому Службою безпеки України та Державною службою спеціального зв’язку та захисту інформації України розроблено та затверджено низку нормативних документів системи технічного захисту інформації.

Одночасно, сьогоденні виклики вимагають змін у питаннях організації заходів із захисту інформації. Нагальним є перехід до ризик-орієнтованих

підходів вирішення питань кіберзахисту комунікаційних та технологічних систем та захисту інформації, яка в них обробляється.

З набранням чинності Законом України «Про основні засади забезпечення кібербезпеки України» реалізувалися положення Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96/2016, зокрема, визначені основні терміни, об'єкти кібербезпеки та кіберзахисту, суб'єкти забезпечення кібербезпеки, а також основні суб'єкти національної системи кібербезпеки та їх основні завдання.

Зазначений закон став підставою для розробки і прийняття Урядом низки постанов Кабінету Міністрів України, зокрема, від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» та від 9 жовтня 2020 р. № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури».

Основні положення інформаційної безпеки держави, яку слід відрізняти від інформаційної безпеки організації (стандарти ISO/IEC 27 серії), викладені у Доктрині інформаційної безпеки України, затвердженій Указом Президента України від 25 лютого 2017 року № 47/2017.

Створення системи інформаційної безпеки розпочалося із затвердження Указом Президента України від 2 січня 2002 року № 63/2002 Положення та Складу Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України. Склад зазначеної комісії було змінено Указом Президента України від 18 червня 2009 року № 462/2009.

Пізніше Указом Президента України від 23 квітня 2008 року № 377/2008 уведено в дію Рішення Ради національної безпеки і оборони України від 21 березня 2008 року «Про невідкладні заходи щодо забезпечення інформаційної безпеки України». Зазначений указ втратив чинність на підставі Указу Президента України від 06 червня 2014 року № 504/2014.

Постановою Кабінету Міністрів України від 16 жовтня 2019 р. № 885 затверджено Положення про Міністерство культури та інформаційної політики України, яким визначено, що МКІП є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику, зокрема, у сфері інформаційної безпеки. Наразі, зазначеним Міністерством розроблено проєкт Стратегії інформаційної безпеки України.

Пріоритетами нормативного врегулювання питань створення систем інформаційної та кібербезпеки держави слід вважати:

Законодавче визначення одного державного органу, відповідального за певний напрямок (МКІП – інформаційна безпека, Адміністрація Держспецзв'язку (Мінцифри) – кіберзахист, Міністерство з питань стратегічних галузей промисловості України – критична інфраструктура). Визначення

інших суб'єктів у визначених сферах та надання визначеному органу права залучати їх до виконання відповідних завдань.

Наділення повноваженнями визначених органів щодо розробки загальних вимог та правил забезпечення безпеки у визначених сферах, які мають бути затверджені відповідним актом Уряду, і які мають стати інструментом для всіх інших суб'єктів у тій або іншій сферах.

Література

1. Закон України «Про основні засади забезпечення кібербезпеки України».

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

3. Указ Президента України від 2 січня 2002 року № 63/2002 «Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України».

4. Указ Президента України від 25 лютого 2017 року № 47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».

УДК 519.85 004.42

Бондарчук С. В.
Галаган В. І.
кандидат військових наук, доцент,
Центр воєнно-стратегічних досліджень
Національного університету оборони України
імені Івана Черняховського

ДЕЯКІ ОСОБЛИВОСТІ ПРОЦЕСУ АВТЕНТИФИКАЦІЇ ТА АВТОРИЗАЦІЇ НА СУЧАСНИХ АНАЛІТИЧНИХ ПЛАТФОРМАХ

Збройні Сили, як і Україна, проходять етап становлення в нових ринкових відносинах. Централізація управління і потреба в розумінні кількісного та якісного стану наявного ресурсу спонукає державу до автоматизації та впровадження централізованих систем обліку та управління [1]. Ефективне використання ресурсів залежить від швидкого збору, оброблення інформації про стан та наявність ресурсів для правильного прийняття ефективного управлінського рішення.

У рамках Плану дій щодо впровадження оборонної реформи у Збройних Силах України [2] та Концепції інформатизації заплановано створення ряду інформаційних систем управління оборонними ресурсами [1-3].

Важливим елементом таких систем є професійно-орієнтована єдина повнофункціональна програмна аналітична платформа (класу Business Discovery) (далі – АП) розміщена на програмно-апаратному комплексі, яка забезпечує вирішення задач користувачів на робочих місцях.

АП використовує аналітичну базу, яка наповнюється даними з різних оперативних джерел. На її основі реалізований автоматизований процес збору та аналітичне оброблення інформації щодо оперативного моніторингу стану справ, визначення проблем, прогнозування і формування необхідної звітності для вищого керівного складу Міністерства оборони України [4].

Для успішного використання можливостей АП необхідно щоб усі посадові особи працювали з однією аналітичною базою, і водночас тільки з тією множиною даних, яка відповідає їх ролі та повноваженням в системі. Важливими елементами такого підходу є *концепції автентифікації і авторизації* в АП.

Автентифікація і авторизація – дві важливі концепції будь-якої АП. Автентифікація гарантує, що людина, яка звертається до системи, є саме тією особою, якою відрекомендовується. Авторизація дозволяє отримати доступ до інформації та здійснювати дії, за якими був налаштований доступ для відповідної ролі.

Сучасні АП використовують два різних процеси, які виконуються незалежно один від одного. Коли користувач отримує доступ до сучасної АП, то завжди виконується 4 кроки. Перші два – це обробка даних web-шаром (АП Server або IIS). На третьому кроці web-шар передає ідентифікаційну інформацію на сервер АП, використовуючи власний протокол. Четвертий крок – це авторизація, яка виконується на сервері АП і використовує групи, дозволені з'єднувачем служби каталогів (далі – DSC).

Важливим елементом авторизації є служба метаданих документів, вона дозволяє давати дозвіл на документи використовуючи Active Directory Groups, а також може давати доступ окремим користувачам.

Перевагами такого підходу є: 1) АП не потрібно зберігати паролі, вони зберігаються у провайдера ідентифікації, таких як LDAP або AD; 2) застосовуються стандартні процедури для управління користувачами, що дозволяє дотримуватися політики безпеки компанії; 3) автентифікація може налаштовуватися за допомогою зовнішніх провайдерів ідентифікації; 4) авторизація проводиться за межами АП, що спрощує захист.

Більшість компонентів АП використовують DSC для авторизації або для отримання інформації про користувачів. Окрім того, в сучасній АП у налаштуваннях аналітичного додатку міститься закритий (закодований) розділ безпеки (Section Access), який використовується для розмежування доступу до даних. Розділ безпеки є частиною скрипта завантаження, де визначається таблиця доступу до даних.

У "живому" додатку, в моделі даних, таблиця авторизації не відображається (вона закодована та прихована від звичайного користувача). Коли посадова особа з конкретним ID користувача відкриває додаток, програма визначає, які поля таблиці клієнтів будуть для нього видимі, а отже і завантажені для аналізу.

У сучасній АП у Section Access передбачено визначення мінімум трьох полів: рівень доступу користувача (ACCESS), ідентифікатор користувача (USERID) і поле усічення, яке вибудовує зв'язок з потрібними даними. Окрім цього, сучасна АП дозволяє враховувати наступні поля: прийнятий пароль (не збігається з паролем операційної системи); серійний номер програми-клієнта; ім'я користувача або групи домену NT; SID домену NT.

Отже, використання даного підходу до авторизації дозволяє сучасній АП, які планується використовувати в діяльності ЗС України організувати усічення даних у різному форматі, а саме: строкового, агрегованого, об'єктного та рівня доступу за полями, що значно спрощує процес доступу до даних.

Література

1. Діджиталізація як основний фактор розвитку бізнесу [електронний ресурс] – Режим доступу: http://confmanagement.kpi.ua/proc/article/view/201186.

2. План дій щодо впровадження оборонної реформи [електронний ресурс] – Режим доступу: https://www.mil.gov.ua/diyalnist/reformi-ta-planuvannya-u-sferi-oboroni/22082016-04.html.

3. Концепція інформатизації Міністерства оборони України [електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0650322-14#Text.

4. С. В. Бондарчук, В. І. Галаган, С. В. Полішко Формування загального обрису інформаційно-аналітичного автоматизованого робочого місця керівного складу управління нерухомим військовим майном Збройних Сил України [електронний ресурс] – Режим доступу: https://doi.org/10.33099/2304-2745/2018-2-63/88-94.

УДК 327.7:061.1(477)

Гуз А.М.
доктор історичних наук, професор,
Національна академія Служби безпеки України

ОСНОВНІ ЕТАПИ СТАНОВЛЕННЯ СИСТЕМИ КІБЕРЗАХИСТУ В ПІВНІЧНОАТЛАНТИЧНОМУ АЛЬЯНСІ НА ПОЧАТКУ XXI СТ.

В умовах протидії гібридній агресії Російської Федерації все більше сучасних країн світу здійснюють мілітаризацію інформаційного простору та розвивають технології його безпеки.

НАТО все частіше стає об'єктом кібернетичних нападів. Саме тому, захист від кібернетичних нападів і готовність протидіяти кіберзагрозам є одним із пріоритетів у діяльності Північноатлантичного альянсу.

Рішення про потребу в розробці комплексної програми з кіберзахисту було прийнято Альянсом у 2002 року. Питання із забезпечення кібербезпеки Північноатлантичного альянсу було предметом обговорення на саміті НАТО у Празі в листопаді 2002 року. Саме тоді розпочалося створення спе-

ціальних органів НАТО, зокрема Агентство НАТО з обслуговування комунікаційних та інформаційних систем, що характеризується як перша лінія захисту Альянсу проти кібертероризму [1].

На Празькому саміту 2002 року було прийнято рішення про створення Сил і засобів реагування НАТО на комп'ютерні інциденти (Computer Incident Response Capability, NCIRC –NATO).

У квітні та травні 2007 року Естонія зазнала серії кібератак [2]. Після цього НАТО дійшла висновку стосовно сприйняття загроз, що виходять з інтернет-простору, як стратегічно важливих. У 2008 р. в м. Таллінні був акредитований Об'єднаний центр передового досвіду з кіберзахисту як центр передового досвіду НАТО (NATO Cooperative Cyber Defence Centre of Excellence). З цього часу Центр став базисом європейської кібербезпеки. Тут щороку у світі проводяться найбільші кібернавчання Locked Shields для експертів у сфері кіберзахисту.

У січні 2008 року міністри оборони країн – членів НАТО схвали офіційну політику Альянсу у сфері кіберзахисту (NATO Cyber Defence Policy) і представили учасникам організації на саміті в Бухаресті у квітні 2008 року.

Сучасне бачення кіберзагроз Північноатлантичним альянсом відображене в Стратегічній концепції, яка була прийнята 2010 році в Лісабоні. Саме у цьому документі інформаційні атаки характеризуються як найбільш небезпечні виклики та загрози безпеці держав-членів Альянсу.

Концепція НАТО з кіберзахисту була розроблена та затверджена під час засідання Північноатлантичної ради на рівні міністрів оборони країн – членів Альянсу у березні 2011 року. Ця концепція визначила захист власних мереж НАТО як головну відповідальність Альянсу у сфері кіберзахисту, необхідність інтеграції кіберзагроз в оборонне планування НАТО, а також наголосила на важливості співпраці з партнерами й іншими міжнародними організаціями. Вона стала основою політики НАТО з кіберзахисту.

Нова політика Альянсу з кіберзахисту (NATO Policy on Cyber Defence) була прийнята 8 червня 2011 р. на зустрічі міністрів оборони країн НАТО. Разом з політикою був узгоджений План дій із кіберзахисту (англ. Cyber Defence Action Plan). Ці документи були офіційно прийняті на саміті НАТО в Чикаго у 2012 році.

Під час Уельського саміту НАТО 2014 року держави – члени Альянсу визнали кіберзахист одним із головних завдань Альянсу.

На Варшавському саміті держави – члени НАТО у 2016 році ухвалили Зобов'язання в галузі кіберзахисту, яке покликане зміцнити й удосконалити кіберзахист національних мереж й інфраструктури [3].

На Брюссельському саміті НАТО у 2018 році було наголошено на важливій ролі кібербезпеки у протидії гібридним загрозам. Члени Альянсу

прийняли рішення нарощувати можливості щодо проведення кібероперацій, зокрема в межах розгортання нового профільного центру (Cyberspace Operations Centre) в Бельгії.

Дослідження показує, що у перше двадцятиріччя XXI століття НАТО ефективно формує свою політику з кіберзахисту. Також варто зазначити, що важливим елементом діяльності НАТО в галузі кіберзахисту на сучасному етапі розвитку є співпраця у мажах Альянсу, а також із міжнародними безпековими організаціями, установами, компаніями.

Література

1. Гуз А. М. Взаємовідносини між НАТО і Україною в 90-ті роки XX ст. на початку XXI ст.// Науковий часопис НПУ імені М.П. Драгоманова. Серія 18. Економіка і право. Випуск 4. – 2006. – С. 131-141.

2. Іноземний досвід правового регулювання охорони державної таємниці: навч. посіб. / Болдир С.В., Гуз А.М., Князєв С.О., Ткачук Т.Ю. та ін. – К.: НА СБУ, 2018. – 160 с. – С.14-15.

3. Міжнародні організації у сфері безпеки. НАТО, ОБСЄ : навч. посіб. / Н. Л. Яковенко ; за наук. ред. В. М. Матвієнка. – К. : ВПЦ Київський університет, 2020. – 367 с. – С.110-111.

УДК 378:477.094

Дашковська О.В.
кандидат хімічних наук, доцент
Погребняк В.П.
кандидат технічних наук, професор,
Інститут модернізації змісту освіти
Міністерства освіти і науки України

МОДЕРНІЗАЦІЯ ВИЩОЇ ОСВІТИ В УКРАЇНІ: ЄВРОІНТЕГРАЦІЙНИЙ АСПЕКТ

З позицій забезпечення конкурентного входження вітчизняної вищої школи в європейський простір вищої освіти оцінюється євроінтеграційна спрямованість процесу імплементації положень Закону України «Про вищу освіту» (далі Закон) [1], яка протягом 2015-2021 років реалізується у вищій освіті України. Для інтеграції в європейський простір вищої освіти Україна, виходячи із загальноєвропейських документів у сфері вищої освіти [2], має досягти основної цілі - забезпечення конкурентоспроможності власної вищої освіти, реформуючи її, застосовуючи для цього такі загальноєвропейські інструменти:

прийняття системи зрозумілих і порівнюваних ступенів вищої освіти;

запровадження структури вищої освіти, яка ґрунтується на трьох циклах (бакалавр, магістр, доктор філософії);

використання ЄКТС як системи накопичення та трансферу освітніх кредитів;

сприяння мобільності студентів, викладачів і науковців;

упровадження додатку до диплома європейського зразка;

визнання попереднього (неформального) навчання;

використання Лісабонської конвенції як основного інструменту визнання кваліфікацій;

розширення автономії університетів, зростання ролі студентства та інших зацікавлених сторін.

З цих позицій оцінимо результати імплементації положень Закону у вітчизняній вищій школі:

1) з урахуванням вимог європейських стандартів суттєво модернізувалась структура вищої освіти. Національна рамка кваліфікацій (далі НРК) частково приведена у відповідність з Рамкою кваліфікацій ЄПВО. Рішенням Уряду у 2020 році [3] НРК була узгоджена з Рамкою кваліфікацій Європейського простору вищої освіти (далі РКЄПВО). Оновлена НРК містить вісім кваліфікаційних рівнів, чотири з яких - рівні вищої освіти;

2) введено в дію новий, наближений до європейського, перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти. Замість 48 галузей знань, 144 напрямів та понад 500 спеціальностей попередніх переліків введено 27 галузей знань і 114 спеціальностей [4];

3) упроваджено стандарт вищої освіти (далі СВО). Він сформований на принципах ЄПВО, визначених Болонським комюніке та міжнародним проектом «Гармонізація освітніх структур в Європі» (Tuning Educational Structures in Europe). Затверджено і введено в дію 98 бакалаврських, 64 магістерських стандартів [5];

4) з 2020року був унормований процес акредитації освітніх програм. Національне агенство із забезпечення якості вищої освіти (далі НАЗЯВО) розглянуло понад 1200 проєктів, акредитувавши біля 700 програм [6];

5) згідно з європейськими стандартами якості та рекомендаціями створена цілісна система забезпечення якості вищої освіти (далі Система якості), яка об’єднує системи внутрішнього забезпечення якості, зовнішнього забезпеченням якості освітньої діяльності та якості освіти і НАЗЯВО [7];

6) НАЗЯВО у порівняно короткий термін стало асоційованим членом ENQA та повноправним членом ще трьох ключових міжнародних організацій у сфері забезпечення якості та академічної доброчесності [8];

7) упроваджено Додаток до диплома про вищу освіту європейського зразка (Diploma Supplement). У ньому міститься інформація, достатня для забезпечення міжнародної зрозумілості отриманої освіти та визнання диплома;

8) розширені автономні права ЗВО: вони самостійно розробляють і затверджують освітні програми, присвоюють наукові ступені, здійснюють

нострифікацію дипломів, отриманих у закордонних закладах, надають грифи навчальній літературі тощо;

9) створено Національний репозитарій академічних текстів - універсальну загальнодержавну електронну базу, в якій накопичуються, зберігаються, систематизуються та аналізуються тексти наукового, науково-технічного та освітнього характеру [9]. Його функціонування сприяє підвищенню рівня академічної доброчесності в освіті і науці та створенню вітчизняної наукометричної системи.

Висновки. В процесі імплементації Закону в Україні вибудовується цілісна система вищої освіти та система забезпечення якості вищої освіти, що робить вітчизняну вищу школу більш конкурентною, наближуючи до європейських критеріїв якості та вимог вітчизняного і міжнародного ринків освітніх послуг.

Література

1. Про вищу освіту:Закон України 1 липня 2014 р. №1556-VII. URL: http://akon2.rada.gov.ua/laws/show/1556-181.

2. The European Higher Education Area. Joint Declaration of Ministers of 5. Bologna), Bologna, Italy, 19 June 1999.

3. Про затвердження Національної рамки кваліфікацій. Постанова КМУ від 23 листопада 2011 р. № 1341. URL: https://zakon.rada.gov.ua/laws/show/1341-2011-%D0%BF#Text.

4. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти». Постанова КМУ від 29.04.2015 р. № 266. URL: http://tntu.edu.ua/nv/files/266.pdf.

5. Затверджені стандарти вищої освіти. URL: https://mon.gov.ua/ua/osvita/visha-osvita/naukovo-metodichna-rada-ministerstva-osviti-i-nauki-ukrayini/zatverdzheni-standarti-vishoyi-osviti.

6. Протоколи засідань. URL: https://naqa.gov.ua/%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D0%B8.-%D0%B7%D0%B0%D1%81%D1%96%D0%B4%D0%B0%D0%BD%D1%8C-%D0%B0%D0%B3%D0%B5%D0%BD%D1%82%D1%81%D1%82%D0%B2%D0%B0/.

7. Погребняк В.П., Дашковська О.В. «Система забезпечення якості вищої освіти». – К.: Знання, «Вища школа», № 3, 2020, с. 82-92.

8. Офіційний сайт НАЗЯВО. URL: http://naqa.gov.ua.

9. Положення про Національний репозитарій академічних текстів. Постанова КМУ від 19. 07 .2017р. № 541. URL: https://www.kmu.gov.ua/npas/250156682.

УДК 65.012.8:339.9
Дзюба Т.М.
кандидат технічних наук, доцент
Деркаченко Я.А.
Опанасенко М.І.
Державний університет телекомунікацій

ОБҐРУНТУВАННЯ КОНЦЕПТУАЛЬНИХ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Збройна агресія Російської Федерації проти України, яка здійснюється з лютого 2014 року, має складний комплексний гібридний характер. Впливи здійснюються як одночасно, так і послідовно, фактично на всі сфери життєдіяльності нашої держави, причому отримані результати в одній сфері відразу використовуються для посилення інших напрямів. Досягнуті результати за різними напрямами гібридної війни демонструються міжнародній спільноті, власному населенню та населенню країни-противника для досягнення загальної мети війни – прийняття противником необхідних умов.

Метою російської "гібридної війни" проти України є утримання України під контролем Російської Федерації та досягнення інших своїх інтересів, використовуючи загрозу збройного конфлікту з Україною. Однією з найважливіших складових цієї війни є інформаційна складова, яка є засобом впливу на рішення воєнно-політичного керівництва; створення необхідних умов для успішних дій збройних формувань (звичайних та іррегулярних); виправдання власних дій та засудження дій противника; мотивації цільових аудиторій до необхідної поведінки; впливу на функціонування систем управління, життєзабезпечення, інфраструктури, транспорту тощо (кіберскладова); мобілізації ресурсів: особового складу для різних складових сектору безпеки і оборони; добровольчих рухів та волонтерської допомоги; різних суб'єктів для безпосередньої участі в інформаційній війні (створення, поширення, знищення, блокування інформації).

Зважаючи на те, що відмова керівництва Російської Федерації від агресивної політики щодо України, в найближчій перспективі, є малоймовірною, Україна потребує створення дієвої та ефективної системи забезпечення інформаційної безпеки.

В Стратегії національної безпеки України основними засадами забезпечення національної безпеки визначені: стримування (розвиток оборонних і безпекових спроможностей для унеможливлення збройної агресії проти України), стійкість (здатність суспільства та держави швидко адаптуватися до змін безпекового середовища й підтримувати стале функціонування, зокрема шляхом мінімізації зовнішніх і внутрішніх уразливостей) та взаємодія (розвиток стратегічних відносин із ключовими іноземними парт-

нерами, насамперед з Європейським Союзом і НАТО та їх державами-членами, Сполученими Штатами Америки, прагматичне співробітництво з іншими державами та міжнародними організаціями на основі національних інтересів України).

Інформаційна безпека є складовою національної безпеки України, отже має базуватись на таких же засадах. Однак, це означає, реактивність нашої інформаційної політики по відношенню до зовнішніх інформаційних впливів.

Іншою проблемою є умовний розподіл на змістовну (контентну) складову інформаційної безпеки, яка визначається, як власне інформаційна безпека та технологічну складову, яка визначається, як кібербезпека. Такий розподіл інформаційної сфери на дві складові разом з реактивністю інформаційної складової національної безпеки не відповідає характеру гібридних загроз, обумовлених російською агресією проти України та особливостями сучасної геополітики.

На наш погляд, концептуальні підходи до забезпечення інформаційної безпеки України мають враховувати:

1. Інтегруючий та системоутворюючий характер інформаційної сфери, оскільки прояви реалізації загроз інформаційній безпеці України можуть спостерігатися в усіх, без виключення, сферах національної безпеки;

2. Необхідність створення системи моніторингу інформаційного простору, яка має функціонувати в безперервному режимі і мати у своєму складі систему раннього виявлення загроз інформаційній безпеці, а також, прогнозування впливу цих загроз на кожну сферу національної безпеки України;

3. Створення єдиного центру прийняття рішень та координації діяльності всіх державних і недержавних інститутів, які відносяться до суб'єктів інформаційної безпеки України;

4. Проактивний характер реагування на загрози інформаційній безпеці України на стадії їх раннього виявлення;

5. Формування базису стійкості до інформаційних впливів, шляхом розвитку національної ідентичності громадян України, збільшення рівня їх медіаграмотності разом зі збільшенням присутності українських інформаційних продуктів в світовому інформаційному просторі, розвитку бренду України, як «гравця» у всіх міжнародних процесах;

6. Узгодження підходів до забезпечення власне інформаційної безпеки (змістовна складова) та кібербезпеки (технологічна складова);

7. Інвентаризації всіх можливостей та ресурсів, які можна залучити для забезпечення інформаційної безпеки України, зокрема можливостей та ресурсів української діаспори в різних країнах світу.

Реалізація зазначених концептуальних положень сприятиме стримуванню збройної агресії Російської Федерації проти України, відновленню територіальної цілісності і державного суверенітету України, своєчасному виявленню і нейтралізації загроз національним інтересам та національній безпеці України в інформаційній сфері, задоволенню національних інтересів України в усіх сферах життєдіяльності нашої держави.

УДК 004.056
Дудикевич В.Б.
доктор технічних наук, професор
Микитин Г.В.
доктор технічних наук, професор
Галунець М. О.
Національний університет «Львівська політехніка»

ОРГАНІЗАЦІЙНІ-ТЕХНІЧНІ АСПЕКТИ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Закон України "Про основні засади забезпечення кібербезпеки України" визначає правові та організаційні основи забезпечення захисту об'єктів критичної інформаційної інфраструктури, які є одним з основних сегментів інтелектуалізації підприємств за концепцією Індустрія 4.0. Безпека інтелектуальних технологій, що забезпечують безпечне функціонування є об'єктів критичної інфраструктури є актуальним питанням кібербезпеки і вимагає зокрема розгляду організаційно-технічних аспектів.

Ефективність безпечного функціонування критичної інформаційної інфраструктури обумовлюється комплексною безпекою критично важливих об'єктів промисловості і довкілля та автоматизованих систем керування процесами і безпровідних комунікаційних систем. Інтелектуалізація критичних об'єктів інфраструктури обумовлює застосування цілого комплексу інтелектуальних систем, сенсорних давачів, що інтегровані в них, а також безпровідних технологій зв'язку, як комунікаційної платформи передавання/приймання даних, відбору інформації від критичного об'єкта та керування його станом.

Безпека функціонування програмно-технічного комплексів критичного призначення за стандартом СОУ – Н НКАУ 0060: 2010 обумовлена їх гарантоздатністю та інформаційною безпекою на рівні загальних властивостей – цілісності і конфіденційності та специфічних – автентичності та достовірності.

Національна система кібербезпеки розгорнута функціональним взаємозв'язком: суб'єктів забезпечення кібербезпеки; об'єктів критичної інфраструктури; технологій підтримки їх безпечного функціонування в організаційному та науково-технічному просторі на основі інтегральних моделей, які, залежно від впливу зовнішніх дестабілізуючих факторів та інформаційних загроз, можуть бути адаптовані до конкретної взаємозв'язаної структури "критичний об'єкт – інтелектуальна технологія" Інтелектуальні об'єкти критичної інфраструктури вимагають проектування безпечних ін-

телектуальних систем, які керують технологічними процесами та моніторингом екосистем довкілля, що на сьогодні є дуже актуальною проблемою безпеки життєдіяльності суспільства в рамках саміту ООН зі зміни клімату (Нью-Йорк, 2019 р.). З цією метою актуальним питанням є функціонування національної системи кібербезпеки у контексті: встановлення вимог до забезпечення інформаційної безпеки об'єктів критичної інфраструктури на етапах їх проектування та експлуатації згідно міжнародних стандартів, розроблення організаційно-технічної моделі заходів і засобів кризового реагування на комплекс кіберзагроз та застосування систем технічного і криптографічного захисту інформації в інтелектуальних і комунікаційних системах. Технічний захист автоматизованих систем і безпровідних технологій підтримки функціонування об'єктів критичної інфраструктури охоплює комплекс систем зовнішнього рівня інтегральної моделі безпеки: відеоспостереження, охоронної сигналізації, контролю доступу, радіочастотної ідентифікації, біометрії. Криптографічний захист інформації, представлений шифраторами і алгоритмічно-програмним забезпеченням – один з ефективних методів забезпечення безпечного відбору інформації від критичних об'єктів, безпечного обміну безпровідними мережами і, на цій основі, прийняття рішення на керування безпекою об'єктів критичної інфраструктури, зокрема екосистемами, транспортом, енергомережами т. і.

УДК 354.32:351.745.5

Ігнатушко Ю.І.
кандидат юридичних наук,
Національна академія внутрішніх справ

ПРИЗНАЧЕННЯ ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ «CUSTODY RECORDS»

Провідна роль у створенні, впровадженні та використанні інформаційних підсистем як міжвідомчого, так і внутрішньовідомчого характеру належить центральним та регіональним підрозділам Національної поліції України. Усе це потребує від співробітників володіння відповідними знаннями та навичками у галузі провідних інформаційних технологій.

Удосконалення діяльності Національної поліції України нині не можливе без надання доступу всім підрозділам правоохоронних органів до єдиного автоматизованого банку даних облікової, оперативно-пошукової, криміналістичної та іншої інформації і забезпечення їхнього диференційованого доступу до цієї інформації[1].

Працівники Національної поліції, які своєчасно оволодівають вірогідною та вичерпною, необхідною їм інформацією, можуть повною мірою

проаналізувати ситуацію, яка склалась, та прийняти правильне рішення стосовно виконання поставленого завдання, що значно підвищує ефективність їхньої діяльності.

Сучасні системи інформаційної безпеки передбачають використання відеоспостереження. Здійснюється відеофіксація того, що відбувається в місцях загального доступу: в аеропортах, вокзалах, на стадіонах, та ін. Використання зображень, отриманих за допомогою систем відеоспостереження забезпечує виконання функцій охорони громадського порядку, безпеки дорожнього руху, захисту власності тощо.

Для належного функціонування суспільства, поліція має повноваження затримувати тимчасово утримувати під вартою і допитувати осіб, підозрюваних у вчиненні кримінальних правопорушень, та інших категорій осіб визначених законодавством. Утім, здійсненню цих повноважень внутрішньо притаманні ризики залякування затриманих та фізичної наруги над ними. Затримані особи перебувають під владою держави, що автоматично накладає на співробітників поліції відповідальність створення безпечних умов тримання цих людей. Держава також зобов'язана врахувати усі загрози та небезпеки, які потенційно можуть виникнути щодо затриманих осіб, як з боку персоналу або інших посадових осіб держави, так і з боку інших затриманих [2].

З метою забезпечення гарантій базових прав затриманих та унеможливлення безпідставних звинувачень у діяльності Національної поліції в Україні запроваджена нова система – «Custody Records».

Завдяки системі «Custody Records» створено новий підхід у ставленні до затриманих осіб.

Відтепер усі відомості та заходи, які пов'язані із затриманням особи, фіксуються в єдиній електронній базі та здійснюється цілодобове відеоспостереження території установи.

Впровадження системи Custody Records створює додаткові гарантії фізичної безпеки людини, її права на життя та особисту недоторканість. Посилений контроль процедури затримання та перебування в місцях обмеження волі, убезпечує особі захист від фізичного або психологічного насилля. Безперервний моніторинг дозволяє оперативно реагувати на екстрені ситуації, запобігати випадкам суїциду, самоушкодженню, тощо.

Основні цілі Custody Records:

- оперативного реагування на порушення прав людини;
- запобігання катувань та інших випадків фізичного та психологічного насильства по відношенню до затриманого;
- запобігання випадків суїциду і самоушкодженню затриманої особи;
- забезпечення захисту співробітників поліції від помилкових звинувачень щодо неналежного поводження;
- фіксація доказів для використання в судочинстві.

Завдання Custody Records:

відстеження порядку тримання та переміщення осіб, забезпечення оперативного реагування на випадки порушень їх прав і законних інтересів;

здійснення інформаційно-пошукових заходів, підготовки аналітично-довідкових матеріалів;

автоматизація процесу обліку затриманих осіб, та формування статистичних даних;

наскрізний контроль (підрозділ контролю, територіальний орган поліції, безпосередній виконавець) за дотриманням прав і законних інтересів осіб під час їх поміщення, тримання та звільнення з ІТТ, своєчасним введенням інформації та її достовірності.

Отже, застосування систем відеоспостереження в місцях несвободи має інший характер в порівнянні з використанням в громадських місцях.

Перед поліцією та контролюючими органами стоїть непросте завдання дотримання балансу між забезпеченням безпеки та недоторканністю приватного життя.

Література

1. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» : Наказ МВС України від 03 серпня 2017 р. № 676.

2. Інформаційні технології в діяльності Національної поліції: навч. посібник. В.А. Кудінов, О.Є. Пакриш, Ю.Ю. Орлов. – НАВС, 2017. 100 с.

УДК 355.40:358.12

Кацалап В.О.
кандидат військових наук, доцент,
Національний університет оборони України
імені Івана Черняховського

ХАРАКТЕРИСТИКА ОСНОВНИХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Критична інфраструктура сучасної держави являє собою складний комплекс різноманітних за своїм характером елементів, який включає низку організаційних структур, різні управлінські моделі, залежні та взаємозалежні функції та системи як у фізичному, так і у віртуальному просторах. Вперше з-поміж "актуальних загроз національній безпеці" відокремлюються загрози критичній інфраструктурі, крім того окремо "Загрози кібербезпеці і безпеці інформаційних ресурсів" йдеться про вразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібе-

ратак. Також з-поміж “основних напрямів державної політики в сфері національної безпеки” розглядається забезпечення безпеки критичної інфраструктури та визначаються пріоритети такого напряму.

Критична інформаційна інфраструктура розглядається як центральний компонент у критичній інфраструктурі різних держав, що знаходить відображення у відповідних визначеннях цього поняття. Головні причини критичності інформаційної складової інфраструктури випливають зі стрімкого поширення інформаційних технологій у всіх сферах людської діяльності, що призводить до залежності від них громадян, суспільства й держави, а також до посилення уразливостей і потенційних загроз різного характеру.

Аналіз поняття інформаційної інфраструктури [1; 2] показав, що вони визначається як сукупність програмно-технічних засобів, інформаційних комунікацій, інших механізмів управління інформаційними ресурсами напрацьованих суспільною практикою, організаційних систем збереження і використання наявних обсягів інформації, а також інститутів продукування нової інформації в інтересах суспільного розвитку, засобів нормативного забезпечення інформаційної діяльності, захисту вітчизняних інформаційних ресурсів від усіх видів загроз та негативних впливів.

Метою тез є проведення аналізу основних об’єктів критичної інформаційної інфраструктури України.

Критична інформаційна інфраструктура розглядається як центральний компонент у критичній інфраструктурі різних держав, що знаходить відображення у відповідних визначеннях цього поняття. Головні причини критичності інформаційної складової інфраструктури випливають зі стрімкого поширення інформаційних технологій у всіх сферах людської діяльності, що призводить до залежності від них громадян, суспільства й держави, а також до посилення уразливостей і потенційних загроз різного характеру.

До об’єктів критичної інфраструктури відносяться підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації, продовольство, охорона здоров’я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв:

провадять діяльність та надають послуги в різних галузях економіки;

надають послуги у сферах життєзабезпечення населення;

включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду;

об’єктами підвищеної небезпеки;

об’єктами, які мають загальнодержавне значення;

об’єктами, порушення функціонування яких призведе до кризової ситуації регіонального значення.

Особливо небезпечними є комбіновані загрози та загрози, реалізація яких може призвести до катастрофічних і різноманітних каскадних ефектів внаслідок взаємозалежності об’єктів критичній інформаційної інфраструктури [3].

Напружена воєнно-політична ситуація, в умовах якої наша держава відстоює власну територіальну цілісність та суверенітет, особливо в рік проведення президентських та парламентських виборів, характеризується значним зростанням рівня загроз зловмисних дій - вчинення терористичних актів та диверсійних операцій на території України, спрямованих на об’єкти критичної інформаційної інфраструктури.

Загрози об’єктам критичній інформаційної інфраструктури можна також розглядати не тільки з точки зору характеру їх походження, але і виділення їх елементів, на які ці загрози спрямовані:

фізичні елементи об’єктів, зокрема, обладнання та ресурси;

системи управління та комунікації, зокрема системи автоматичного управління та регулювання роботи об’єктів, системи зв’язку тощо;

персонал об’єктів, зокрема диспетчерський, оперативний персонал, який безпосередньо забезпечує функціонування об’єктів у реальному часі.

Таким чином, розглянувши характеристики основних об’єктів критичної інформаційної інфраструктури, можна зробити висновки, що об’єкти критичної інформаційної інфраструктури в нашій державі, особливо в умовах ведення проти нас Російською Федерацією “гібридної війни” потребують впровадження новітніх технологій та залучення значних ресурсів і коштів для їх захисту незалежно від форми власності того чи іншого об’єкту.

Література

1. Розпорядження Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р “Про ухвалення Концепції створення державної системи захисту критичної інфраструктури”.

2. Бірюков, Д. С. Зелена книга з питань захисту критичної інфраструктури в Україні [Текст] /Д. С. Бірюков, С. І. Кондратов, О. М. Суходоля. – К.: НІСД, 2015.

3. Dennis M.Murphy. Strategic Communication Talking the Talk: Why Warfighters Don’t Understand Information Operations / Center for Strategic Leadership; U.S. Army War College. 2009. May. Volume 4-09.

УДК 004.056
Козюра В.Д.
кандидат технічних наук, доцент
Бровко В.Д.
кандидат технічних наук,
Національна академія Служби безпеки України

ОСОБЛИВОСТІ СУЧАСНИХ КІБЕРАТАК

У 2019 р. кількість кібератак у світі перевищило 2,25 млн. (атаки здійснювалися кожні 14 с). Зі збільшенням числа кібератак зростає і заподіяна ними шкода: в 2018 р. збитки підприємств склали $1,5 трил., в 2019 р. - $2,5 трил., а до 2022 р., за прогнозом Світового економічного форуму, сума планетарної шкоди від кібератак може вирости до $8 трил. Що таке кібератака? Закон України «Про основні засади забезпечення кібербезпеки України» визначає кібератаку як «спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту».

Тому для підвищення рівня кібербезпеки сучасних інформаційно-телекомунікаційних систем, що використовуються, у першу чергу, в сферах критичної інфраструктури держави, необхідно розуміти всі кроки розвитку кібератаки з точки зору її виявлення і захисту.

На першому кроці порушник здійснює зовнішню розвідку – шукає уразливу жертву для атаки. Збирається інформація про уразливості за межами мережі організації, яка дозволить порушникові вибрати методи експлуатації, відповідні для кожної уразливості, визначеної для конкретної цілі. На цій стадії зазвичай використовуються два методи: фішинг за допомогою електронних листів і соціальна інженерія. Після використання цих методів порушник знайде точку входу. Це може бути зроблено за допомогою крадіжки паролів або зараження комп’ютера шкідливим ПЗ в мережі цільової організації.

На другому кроці – скануванні – порушник досліджує слабкі місця ІТС, виявлені на етапі розвідки. Сканування включає використання різних інструментів, щоб знайти лазівки, які можна використовувати для організації атаки. В якості доступних інструментів сканування можуть використовуватися наступні:

- NMap - мережева утиліта з відкритим початковим кодом для Windows, Linux і macOS, що використовує звичайні IP-пакеты (виявляє пристрої, підключені до цільової мережі, та їх відкриті порти; відстежує час роботи хостов в мережі; з'ясовуються сервіси, працюючі на хостах; ідентифікуються ОС, використовувані хостами; визначаються правила брандмауера, вживані в мережі); .
- Metasploit - фреймворк для злому на базі Linux, що надає важливу інформацію про численні уразливості й методи їх експлуатації (за допомогою эксплойтів);
- John the Ripper - автономна утиліта для злому паролів в ОС Linux і Windows, яка використовується для здійснення словникових атак. Застосовується для витягання реальних паролів користувачів із зашифрованих баз даних як персональних комп'ютерів, так і веб-систем і застосувань;
- THC Hydra - онлайн утиліта злому паролів в ОС Windows, Linux і macOS X. Використовує словникові атаки і повний перебір для атаки на сторінки входу;
- Wireshark - утиліта сканування мереж збирає пакети даних в цільовій мережі, відображає їх в детальному форматі, зручному для читання, і дозволяє фахівцям ретельно аналізувати мережевий трафік до рівня перевірки окремих пакетів;
- Aircrack-ng - набір інструментальних засобів, використовуваний для злому ключів безпровідних мереж. Він включає такі атаки, як FMS (отримання ключів, які були зашифровані з використанням RC4), KoreK (атаки на мережі Wi-Fi, які захищені паролями з WEP-шифруванням) і PTW (злом захищених мереж Wi-Fi з шифруванням WEP і WPA);
- Nikto - сканер уразливостей веб-сайтів на основі Linux. Утиліта сканує веб-сервери на наявність понад 6800 експлуатованих уразливостей, а також сканує версії серверів, в яких не виправлені уразливості на більш ніж 250 платформах. Він також перевіряє наявність помилок в конфігураціях файлів на веб-серверах;
- Cain and Abel - утиліта для злому паролів, яка ефективна проти ОС Microsoft. Зламує паролі, використовуючи словникову атаку, повний перебір і криптоаналіз. Дозволяє записувати розмови, які йдуть через VOIP, розшифровувати паролі, розкривати кешировані паролі і аналізувати протоколи маршрутизації внутрішньої мережі.

Третій крок атаки – доступ і підвищення привілеїв. Основними завданнями порушника є збереження доступу і переміщення по мережі, залишаючись при цьому непоміченим. Для цього порушникові необхідно виконати підвищення привілеїв, яке може бути виконане двома способами: вертикальним (порушник переміщається з одного акаунта на інший з вищим рівнем повноважень) і горизонтальним (порушник використовує той же обліковий запис, але підвищує свої привілеї).

Четвертий крок – проникнення і витоки – з цього кроку починається основна атака: порушник може безперешкодно пересуватися по мережі, маючи доступ до усіх її систем і таємних даних. На цьому етапі порушники крадуть величезні масиви даних, які можуть бути або продані, або опубліковані.

Якщо порушники припускають протягом тривалого часу здійснювати крадіжку конфіденційної інформації, то атака переходить до п'ятого кроку, умовно названого «тилове забезпечення». Порушники встановлюють шкідливі програми, такі як руткити, які забезпечують ним доступ до комп'ютерів і систем жертви у будь-який час. Головна мета входу в цю стадію - виграти час, щоб підготуватися до більш небезпечної ніж витік атаці на обладнання організації.

Шостий крок атаки – штурм – найнебезпечніша стадія будь-якої кібератаки, бо порушник завдає збитки апаратним засобам. Він може назавжди відключити або змінити роботу устаткування, фокусується на знищенні апаратного забезпечення, керованого скомпрометованими системами. Наочним прикладом атаки, яка досягла цього кроку, є атака Stuxnet на іранську атомну станцію. Це була перша зареєстрована цифрова зброя, яка використовувалася для руйнування фізичних ресурсів.

Заключним сьомим кроком атаки є обфускація (маскування), мета якої полягає в тому, щоб порушники приховали сліди свого перебування в мережі жертви. Для цього використовуються різні методи з метою заплутати, утримати або відвернути процес розслідування, який йде за кібератакой.

Що цьому можна протиставити? Очевидно, основною метою забезпечення кібербезпеки сучасних ІТС є нейтралізація кібератак на самих ранніх стадіях їх розвитку. Для цього необхідно здійснювати постійний збір даних про сучасні кіберзагрози в усіх сферах ІТ-інфраструктури, виявляти актуальні кіберзагрози і класифікувати їх з метою виявлення потенційної небезпеки, своєчасно проводити ретельне розслідування актуальних атак, нейтралізувати їх впливи на організацію і в найкоротші терміни відновлювати працездатність системи. Це і становить суть сучасної парадигми кібербезпеки – керування життєвим циклом кібератак.

УДК 654.1
Котенко А.М.
кандидат технічних наук, доцент
Гребенніков А.Б.
Державний університет телекомунікацій

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Технічні системи охорони використовуються у кібербезпеці як засіб запобігання витоку інформації матеріально-речовим каналом. Пропонується використовувати метод динамічного програмування для побудови ефективної технічної системи охорони з метою підвищення ефективності захисту кібернетичної безпеки об'єкту інформаційної діяльності.

Характерною проблемою сьогодення є забезпечення безпеки інформації. Виходячи з цього стає більш актуальнішою необхідність забезпечення кібернетичної безпеки об'єктів інформаційної діяльності. Одним з засобів забезпечення кібернетичної безпеки є технічні системи охорони об'єктів [1]. Вони захищають інформацію від витоку матеріально-речовим каналом. На сьогодні під час проектування таких систем наукові підходи не використовуються. Під час проектування лише суб'єктивно оцінюється вартість складових, їх характеристики і не більше.

Пропонується використовувати метод динамічного програмування для побудови ефективної технічної системи охорони.

Динамічне програмування в теорії управління і теорії обчислювальних систем - спосіб вирішення складних завдань шляхом розбиття їх на більш прості підзадачі. Він застосовується до завдань з оптимальною підструктурою, що виглядає як набір перетинающихся підзадач, складність яких трохи менше вихідної. У загальному випадку алгоритм вирішення задачі, в якій присутня оптимальна підструктура, виглядає так [2]:

1. Розбиття задач на підзадачі меншого розміру.

2. Знаходження оптимального рішения підзадач рекурсивно, проробляючи такий же трьохкроковий алгоритм.

3. Використання отриманого рішення підзадач для конструювання рішения вихідної задачі.

Технічна система охорони (ТСО) складається з наступних елементів: сповіщувачі (чутливі елементи), прилад прийомо-контрольний (ППК). Виходячи з цього у математичному вигляді постановка завдання на вибір оптимального варіанту системи буде виглядати наступним чином.

Дано: (X1 – сповіщувачі; X2 – ППК) – система *K*.

Знайти: *K*→ optim за критерієм (цільова функція):

$$\max\left(\frac{F}{I}\right) = \max\left(\frac{\sum_i f_i}{\sum_i I_i}\right) \quad (1)$$

де:

F – показник корисності *i* – ої реалізації технічної системи охорони;

I – вартість і – ої реалізації технічної системи охорони.

У відповідності з методом динамічного програмування буде розраховано показник корисності кожної складової системи *К*. Далі методом повного перебору буде прораховано значення цільової функції для кожної реалізації ТСО. Усього кількість таких реалізацій ТСО буде:

$$N = \prod_{i=1}^{n} K_i$$

де:

n – число елементів ТСО;

K – число альтернатив кожного елементу ТСО.

Для розрахунку показників корисності обираються сповіщувачі та ППК, що будуть використовуватися і визначаються їх найбільш важливі показники якості. Далі за виразами лінійної трансформації [3] здійснюється нормування цих показників. Якщо відповідному показнику якості x_1 більш максимальне значення відповідає більш якісній роботі, то вираз переходу від ненормованого значення показника x_nдо нормованого має вигляд:

$$X_n = \frac{x_1 - f_1^{min}}{f_1^{max} - f_1^{min}}$$

де:

f_1^{min} і f_1^{max} – відповідно абсолютні мінімальне (найгірше) й максимальне (найкраще) значення показника якості роботи серед усіх варіантів;

x_1 – абсолютне значення показника, що нормується.

Якщо для деякого показника x_1 абсолютне мінімальне значення відповідає більш якісному функціонуванню, то вираз трансформації матиме вигляд:

$X_n = \frac{f_1^{max} - x_1}{f_1^{max} - f_1^{min}}$.

Далі визначаються вагові коефіцієнти показників якості елементів ТСО. Дуже поширеним і простим, наприклад, є метод експертного оцінювання.

За виразом (2) розраховується показник корисності f_i для кожного елементу ТСО:

$$f_i = \sum a_i Kc_i \quad (2)$$

де:

a_i – вага показника якості елементу ТСО;

Kc_i – нормоване значення показника якості відповідного показника якості.

За формулою повного перебору визначається кількість варіантів побудови ТСО. Розраховується вартість усіх можливих реалізацій ТСО. Розраховується показник корисності кожної реалізації як сума нормованих показників корисності усіх складових ТСО у даній реалізації. За виразом (1) обчислюється значення функції для кожній реалізації ТСО. З них обирається найкращий варіант реалізації системи.

Література

1. Котенко А.М. Запобігання витоку інформації матеріально-речовим каналом за рахунок використання систем відеоспостереження. Сучасний захист інформації. Київ: ДУТ, 2017. № 1. – С. 48–52.

2. Кулич И.Л. Глава 4. Задачи динамического программирования // Математическое программирование в примерах и задачах. – М.: Высшая школа, 1986. – 319 с. – ISBN 5-06-002663-9.

3. https://psytest.wordpress.com/data_treatment/normalization_indicator/.

УДК 378:477.094

Котович В.М.
Інститут модернізації змісту освіти
Міністерства освіти і науки України

ЕТИЧНЕ ТЕСТУВАННЯ НА ЗЛОМ ТА ПРОНИКНЕННЯ

Що таке етичне тестування на злом та проникнення?

Етичний хакер - це експерт з інформаційної безпеки, який систематично намагається проникнути в мережу або комп'ютерну систему чи мережу, щоб виявити вразливі місця безпеки, якими зловмисний хакер може зловживати. Ця робота вимагає подібного набору навичок, як зловмисний хакер, наприклад:

Розсилка фішинг-листи (Send phishing emails).

Грубі атаки підбору паролю (Brute-force password attacks).

Периметральні порушення (Breach perimeters).

Вразливості неправильної конфігурації системи (Exploit system misconfigurations).

Зазвичай наймають етичних хакерів до того, як нова система почне діяти, і часто організації використовують схему винагороди: фінансова винагорода надається етичним хакерам, які демонструють докази вади системи.

Тестування на проникнення - це специфічний тип етичного злому, який передбачає наймання сертифікованого професіонала для оцінки достоїнств вже існуючої системи. Зазвичай пен тестери отримують привілейовану інформацію та використовують її для виявлення недоліків, які можна використати. Ці тести включають:

Тести веб-додатків.

Тести бездротової мережі.

Тести зовнішньої / внутрішньої мережі.

Ці пен тести, як правило, є більш систематизованими та проводяться у звичайний, заданий час, тобто до того, як буде випущена серйозна зміна програми.

Чи законний етичний злом?

Етичний злом існує в цікавій юридичній сірій зоні. Деякі закони щодо етичного злому неоднозначні або не враховують усіх сценаріїв, з якими стикається етичний хакер.

Основна відмінність між етичним та неетичним злом - це згода. Хакер повинен мати дозвіл діяти, а організація повинна мати дозвіл клієнта на видачу конфіденційних даних.

Найкращий спосіб захистити сторони - це підписати юридичну угоду, яка відповідає наступним чотирьом умовам:

Заява про роботу (SOW) підписується як хакером, так і клієнтом. Це описує мету злому та те, які дії хакеру дозволено робити.

Для захисту ділової інформації підписується NDA.

Обидві сторони мають повну прозорість щодо очікувань та всіх вжитих дій.

Обидві сторони підписують форму звільнення від відповідальності, щоб звільнити хакера від будь-якої відповідальності за ненавмисні результати.

Види хакерів та термінологія

Отже, ми знаємо, що етичні хакери використовують навички зловмисного хакера, щоб допомогти компанії. Але як щодо інших типів хакерів? Давайте дослідимо різні типи хакерів і дізнаємось, чим вони відрізняються від етичних хакерів.

Білі хакери

Також їх називають етичними хакерами, це професійні фахівці / аналітики з питань безпеки та тестери проникнення, які співпрацюють з компаніями, галузями та комп'ютерними системами для розробки більш надійних систем безпеки. Вони повинні розуміти методологію зловмисних хакерів, а

також існуючі законодавчі рамки, що визначають поточні протоколи безпеки.

Чорні хакери

Це злісні хакери, які використовують слабкі місця для вигоди. Це люди, яких ми хочемо зупинити. Вони є хакерами, які шукають порушення даних зі зловмисними намірами, наприклад, розповсюдження шкідливих програм / вірусів та зловмисний аналіз даних. Хакери "чорних капелюхів" часто здійснюють банківські шахрайства, вимагання, шантаж та крадіжку особистої інформації щодо користувачів мережі.

Сірі хакери

Ці хакери можуть не використовувати дані для збитків, але вони використовують неетичні засоби, щоб зробити систему безпечнішою. Хакери з сірими капелюхами розуміють тонкощі хакерства і можуть використовувати їх для самообслуговування. Наприклад, несанкціонований хакер проникає на веб-сайт і надсилає електронний лист технічному директору про виявлену ними слабкість. Ні, вони нікому не шкодять. Але так, вони порушують закон.

Зелені хакери

Це хакери з обмеженим розумінням процесу і можуть використовувати очевидні методи для злому приватних даних та паролів. Їх зазвичай можна знайти в соціальних мережах, особливо на форумах в Інтернеті, щоб затримати нічого не підозрюючих користувачів.

Сині хакери

Ці хакери, як правило, зловмисні щодо однієї компанії чи людини. Хакери цієї групи використовують свої навички для експлуатації конкретних людей з метою помсти. Хакер блакитного капелюха може мати політичну мотивацію.

Червоні хакери

Це пильні хакери. Ці хакери намагаються зупинити зловмисних хакерів за допомогою таких речей, як віруси, ініціювати DoSing або навіть знищити комп’ютер зсередини. Їх надмірні методи спрямовані на те, щоб повністю закрити чорного хакера.

Скриптовики

Це хакери, які мають дуже обмежені практичні знання щодо злому, але навчаться проникати в мережеві системи. Можливо, вони шукають дані з різних архітектур і покладаються на заздалегідь написаний код або програмне забезпечення для проникнення в мережу.

Література

1. Quora.
2. CyberSecurityMastersDegree.
3. Zakon.rada.gov.ua.

УДК 004.056
Криворучко О.В.
доктор технічних наук, професор
Десятко А.М.
Київський національний торговельно-економічний університет
Сунічук О.М.
ТОВ «Новелл Консалтинг»

МОДЕЛЮВАННЯ ІУС НЕЗАЛЕЖНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Однією з проблем сьогодення є поширення та масштаби кіберзлочинності не лише в Україні, а й у світовому масштабі. Завдання держави полягає у підготовці фахівців, які б спрацьовували на випередження кіберзлочинів, із врахуванням досвіду інших країн. Також ця проблема спонукає до вдосконалення та трансформації норм, що регулюють суспільні відносини у кібепросторі. В світі має вдосконалюватись підготовка фахівців з ІТ-аудиту або кібеаудиту. Фахівці по боротьбі з кібезагрозами та кібершахрайствами мають бути постійно обізнані в розвитку ІТ-новинок і ризиків, які можуть виникнути під час несанкціонованих вторгнень в систему. В сучасних умовах до професійної підготовки фахівців існують певні вимоги, які розкриваються через таке поняття, як модель спеціаліста, тобто професійно-обумовлена структура особистості в освітньому процесі. Як правило це вже є процес підвищення кваліфікаційного рівня фахівця.

Як наслідок, важливе значення має модель ІУС аудиту інформаційної безпеки. На процес моделювання ІУС аудиту інформаційної безпеки впливає інтеграція зовнішньої і внутрішньої інформації, горизонтальна та вертикальна інтеграція між системами з різною ієрархічною структурою [1].

Визначені наступні принципи моделювання: принцип кінцевої мети; принцип єдності; принцип зв’язку; принцип модульної побудови; принцип ієрархії; принцип функціональності; принцип розвитку; принцип децентралізації; принцип невизначеності [1].

Моделювання передбачає проведення розрахунків, спостережень, логічного аналізу на моделях з тим, щоб за результатами такого дослідження можна було судити про явища, які відбуваються в реалії [1].

На основі запропонованих моделей є можливість створювати раціональні технічнопрограмні засоби [1]. При моделюванні ІУС незалежного аудиту інформаційної безпеки важливе значення мають впливи зовнішніх факторів. Серед них найважливіше місце займає нормативна база.

Потрібно відмітити, що важливе місце при реалізації моделі ІУС незалежного аудиту інформаційної безпеки складає державно-приватне партнерство, що дозволяє покрити підприємства різного типу та визначеного доступу.

Прийняття Верховною Радою 5 жовтня й підписання Президентом України 7 листопада 2017 року Закону України «Про основні засади забезпечення кібербезпеки України» [2], а також затвердження Указом Президента України (від 15 березня 2016 року № 96/2016) "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [3] заклали основи національного галузевого законодавства і визначили ключові вектори його подальшого розвитку відповідно до європейських демократичних практик. В обох документах значущу увагу приділено питанню правового регулювання державно-приватного партнерства у забезпеченні кібербезпеки.

Протягом останніх 5 років термін «державно-приватне партнерство» (запозичений з англійської «private-public partnership», або скорочено «PPP») очолює рейтинг популярності у словниковому запасі українських держлужбовців. Цей термін спонукає на ефективну співпрацю між державним апаратом та бізнесом, який спрямовану на залучення не лише приватних інвестицій у державну інфраструктуру, а й інтелектуальний потенціал практиків та науковців.

Державно-приватне інтелектуальне партнерство це поєднання зусиль держави та бізнесу у сфері інформаційної безпеки, яке має важливе значення, але при цьому має й певні ризики, як все нове. Кожна зі сторін партнерства отримує свої переваги у процесі реалізації проєктів. Для державних структур переваги вбачаються у можливості залучення приватних партнерів-практиків та науковців для реалізації проєктів, які є важливими, однак з високою долею ймовірності залишалися б нереалізованими протягом тривалого періоду часу через нестачу кадрового забезпечення напряму інформаційної безпеки. Переваги для бізнесу та науки полягають у державній підтримці шляхом надання можливості для впровадження новітніх наукових розробок (методик, програного забезпечення та ін.) Для державного сектору - доступі інтелектуальні та практичні розробки фахівців практиків та науковців (наукові дослідження в сегменті інформаційної безпеки, нові методичні підходи щодо забезпечення для апаратно-програмного комплексу системи оцінки фахової підготовки аудиторів інформаційної безпеки, збору та аналізу інформації, отриманої під час аудиту інформаційної безпеки) .

Література

1. Криворучко О.В. Моделювання інформаційної системи проведення незалежного аудиту інформаційної безпеки [Текст] / О.В. Криворучко, А.М. Десятко, О.М. Сунічук // Управління розвитком складних систем. – 2020. – № 43. – С. 67–75.

2. Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403).

3. 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.

УДК 621.3

Крючкова Л.П.
доктор технічних наук, доцент
Вовк М.О.
Державний університет телекомунікацій

ДОСЛІДЖЕННЯ ПАРАМЕТРІВ ПРИЦІЛЬНИХ ЗАВАДОВИХ СИГНАЛІВ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Особливе місце в соціальній інфраструктурі будь-якої держави займають об'єкти критичної інфраструктури. Порушення функціонування таких об'єктів може мати руйнівний характер, тому заходи з протидії зловмисним діям повинні повною мірою перекривати загрози і вразливості інформаційної безпеки [1]. Важливим завданням на об'єктах критичної інформаційної інфраструктури є унеможливлення перехоплення конфіденційної інформації, що забезпечується блокуванням технічних каналів витоку інформації.

Ефективними методами перехоплення акустичної інформації є метод формування небезпечних сигналів радіозакладними пристроями та метод високочастотного нав'язування.

Відомий метод блокування сигналу перехоплення інформації методом високочастотного нав'язування [2], сутність якого полягає в застосуванні комбінованої активної завади (захисний сигнал), спрямованої на руйнування інформативних параметрів небезпечного сигналу.

Мета наших досліджень полягала у знаходженні параметрів захисних сигналів, здатних забезпечити максимально можливу руйнацію інформативних параметрів небезпечного сигналу, і, як результат, створення протидії перехопленню конфіденційної інформації зацікавленими особами.

Для виконання досліджень використовувались методи математичного та імітаційного моделювання. В результаті теоретично розраховано та методами імітаційного моделювання практично визначено максимально ефективні параметри захисних сигналів, які в перспективі можна використовувати в системах автоматичної радіопротидії небезпечним сигналам різноманітного походження.

Фрагмент результатів моделювання сигналів наведено на рисунку 1.

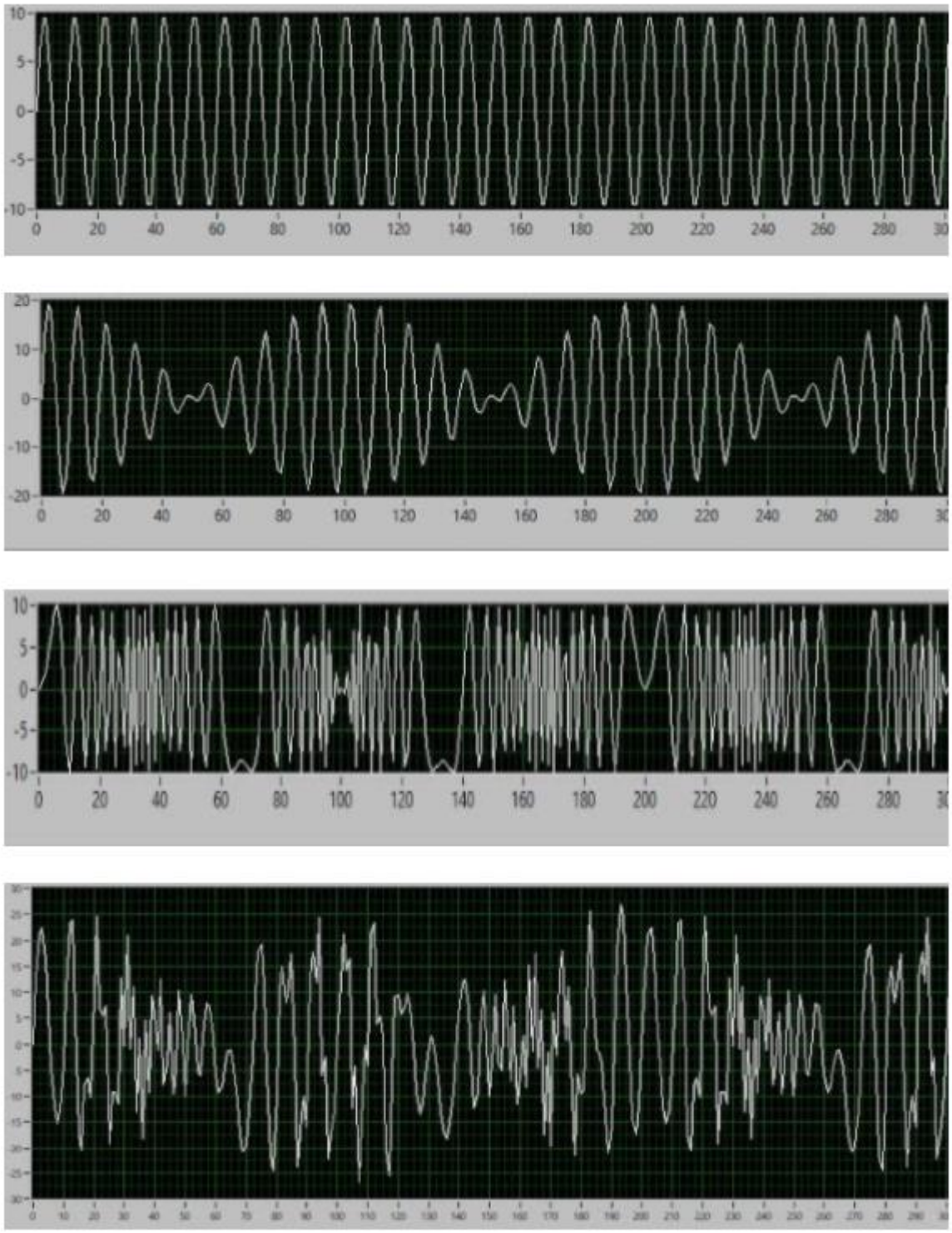


Рис. 1. Зображення сигналів
(а - небезпечний сигнал, б - сигнал биття, в - сигнал коливальної частоти, г - результуючий небезпечний сигнал)

При виявленні засобами радіомоніторингу на об’єкті небезпечного сигналу засобами захисту формується захисний сигнал, здатний зруйнувати інформативні параметри небезпечного сигналу.

Спираючись на результати досліджень можна сказати, що для досягнення поставленої мети, захисний сигнал повинен складатися з двох сигналів: несучої, з частотою, віддаленою на 10% від частоти небезпечного сигналу для створення ефекту биття, та сигналу коливальної частоти в межах від 5% до 20% частоти небезпечного сигналу.

В доповіді наводяться результати математичних розрахунків, виконаних з використанням мови програмування Python та імітаційного моделювання впливу прицільних завадових сигналів на інформативні параметри небезпечних сигналів з використанням пакету LabVIEW версії 20.0.1.

Література

1. Про критичну інфраструктуру та її захист. Проект закону України від 27.05.2019 №10328. [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/JH7YW00A.html.

2. Патент 95365 Україна, МПК (2011.01) H04K 3/00. Спосіб захисту інформації / Рибальський О.В., Хорошко В.О., Крючкова Л.П., Джужа О.М., Орлов Ю.Ю.; заявник і патентовласник Національна академія внутрішніх справ. - № a200913327; заявл. 22.12.2009; 55 опубл. 25.07.2011, Бюл. № 14.

УДК 681.51

Крючкова Л.П.
доктор технічних наук, доцент
Тарасенко Д.О.
Державний університет телекомунікацій

ІНФОРМАЦІЙНЕ ТА АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ СИТУАЦІЙНОГО УПРАВЛІННЯ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ДЕСТРУКТИВНИХ ВПЛИВІВ

Згідно з [1] до завдань формування і реалізації державної політики захисту критичної інфраструктури України і створення державної системи захисту критичної інфраструктури належать забезпечення безпеки, стійкості та цілісності критичної інфраструктури України; попередження кризових ситуацій, що порушують стале функціонування критичної інфраструктури. Актуальним при цьому є створення умов, спрямованих на мінімізацію реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів; створення умов швидкого відновлення функціонування критичної інфраструктури у випадку реалізованих загроз, кризових ситуацій; створення системи виявлення загроз критичній інфраструктурі.

Загрози критичній інфраструктурі можуть бути спрямовані на *системи управління та комунікації* об'єктів критичної інфраструктури, зокрема системи автоматичного управління та регулювання роботи об'єктів, системи

зв'язку тощо [2]. Проблемою, яка представляє інтерес для дослідження, є забезпечення інформаційної підтримки антикризового управління для прийняття управлінських рішень з метою підвищення обґрунтованості, достовірності та ефективності при вирішенні завдань антикризового управління.

Аналіз можливостей використання традиційних підходів до управління, заснованих на методах оптимізації і адаптивного управління, для розглянутого класу складних об'єктів в умовах завад і кризових ситуацій показують, що їх можливості обмежені через необхідність використання повної і точної математичної моделі об'єкта. Методи штучного інтелекту (нечітка логіка, нейронні мережі, генетичні алгоритми, експертні системи) мають свої сильні сторони і дозволяють знайти рішення в багатьох конкретних застосуваннях. Однак найбільш перспективним для антикризового управління вважається *ситуаційний підхід,* який надає можливість гнучкого відстеження і прогнозування поведінки складного об'єкту та адаптивного управління ним у різних ситуаціях.

В доповіді обґрунтовується підхід до вирішення проблеми завадостійкого ситуаційного управління на основі аналізу ситуації і прийняття управлінських рішень (рис.1). Обговорюються особливості ситуаційного управління, причини, наслідки, рішення і резерв часу в кризових ситуаціях в умовах невизначеності, обумовлених деструктивними впливами. В рамках цього підходу формулюється мета дослідження і визначаються основні завдання, які необхідно вирішити для досягнення мети.

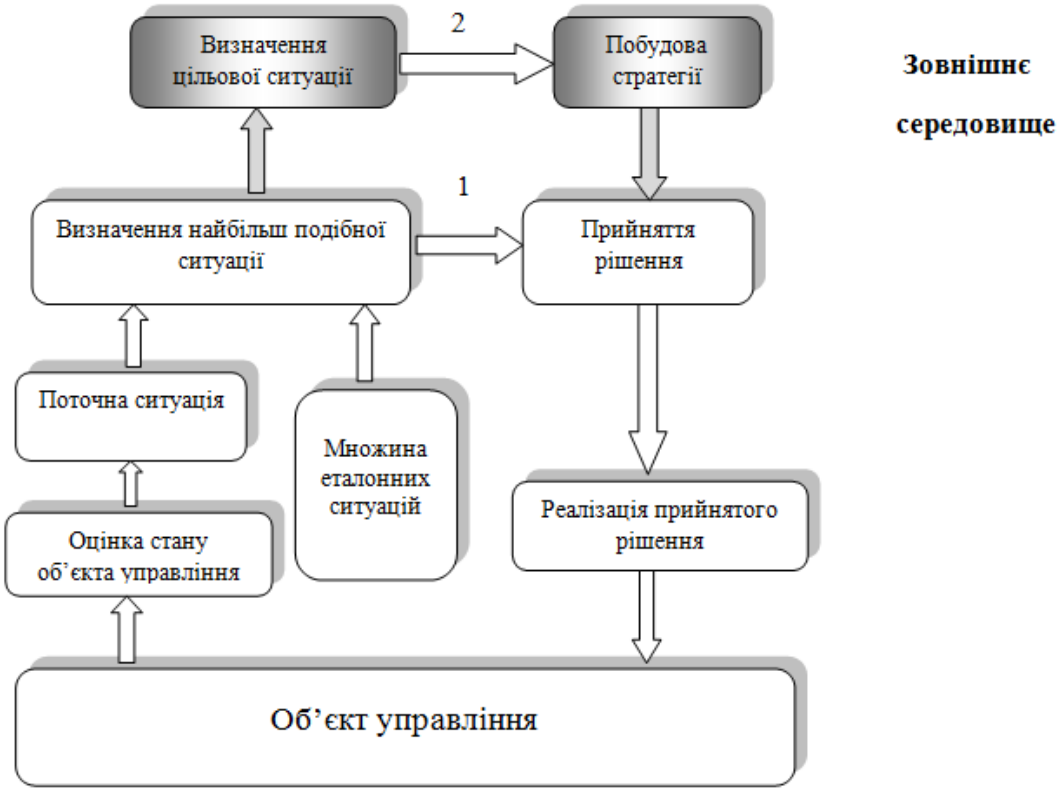


Рис.1. Блок-схема ситуаційного управління

Кризова ситуація розглядається як наслідок змін характеристик системи в результаті порушень (відмов, зовнішніх впливів, помилок управління), яка в разі неприйняття своєчасних і цілеспрямованих заходів з управління може призвести до небажаних наслідків з неприпустимо великими втратами.

Для кожної еталонної ситуації ставиться у відповідність цільова ситуація s_i^c , $s_i^c \in S_c$, де S_c – множина цільових ситуацій, $S_c \subseteq S$. Крім того, в системі ситуаційного управління зберігається (або створюється в процесі пошуку рішень) ситуаційна мережа – орієнтований граф переходів по ситуаціях під впливом прийнятих рішень.

Новизна інформаційно-алгоритмічного забезпечення ситуаційного управління в умовах деструктивних впливів обумовлена новизною об'єктно-орієнтованої ієрархічної ситуаційної моделі, яка на базі об'єктно-орієнтованого підходу об'єднує інформаційні структури моделі і алгоритми їх інтерпретації для організації процесу управління.

Запропоновані алгоритми ситуаційного аналізу дозволяють врахувати динаміку і особливості розвитку ситуацій в умовах деструктивних впливів як на рівні окремих ізольованих ситуацій, що виникають в процесі функціонування складного об'єкту, так і на рівні системи управління з урахуванням ситуаційної взаємодії.

Література

1. Про критичну інфраструктуру та її захист. Проект закону України від 27.05.2019 №10328. [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/JH7YW00A.html (дата звернення: 4.03.2021).

2. Бірюков Д.С., Кондратов С.І., Насвіт О.І., Суходоля О.М. Зелена книга з питань захисту критичної інфраструктури в Україні. –К: Національний інститут стратегічних досліджень, 2015. – 35 с.

УДК 621.396

Крючкова Л.П.
доктор технічних наук, доцент
Українець Є.О.
Державний університет телекомунікацій

ДОСЛІДЖЕННЯ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ІНТЕРФЕЙСУ USB В СТРУКТУРІ СИСТЕМ УПРАВЛІННЯ ОБ'ЄКТАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Одним з ключових напрямків розвитку сучасного суспільства є формування інтегрованого інформаційного простору на основі новітніх інформа-

ційних технологій. 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. Під критичною інфраструктурою розуміють сукупність об'єктів, які є стратегічно важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

Об'єкт критичної інфраструктури – визначений у встановленому законодавством порядку складовий елемент критичної інфраструктури, функціональність, безперервність, цілісність і стійкість якого забезпечують реалізацію життєвоважливих послуг та функцій [1].

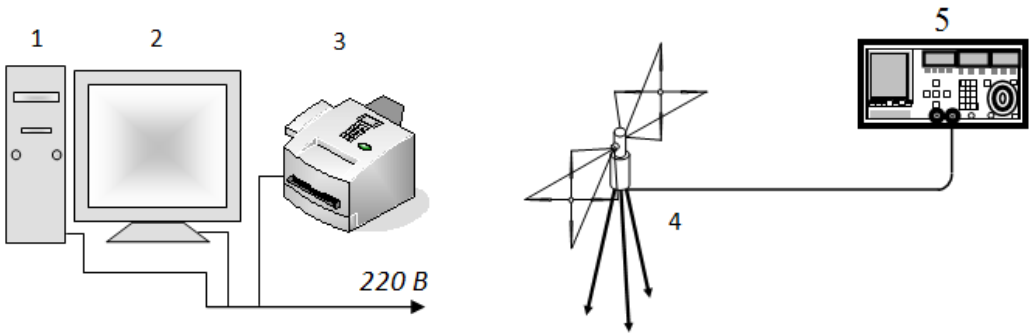
Важливим елементом кіберзахисту об'єктів критичної інформаційної інфраструктури є забезпечення належного рівня державно-приватного партнерства органів державної влади та підприємств сфери інформаційно-комунікаційних технологій України. З урахуванням обмеженості фінансових та кадрових ресурсів держави для підтримки функцій кібербезпеки саме державно-приватне партнерство має стати основою підвищення ефективності забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури.

Одним з можливих каналів витоку інформації є випромінювання елементів комп'ютера, точніше, елементів основних технічних засобів, якщо говорити про захищені автоматизовані системи. Приймаючи і декодуючи ці побічні електромагнітні випромінювання, можна отримати відомості про інформацію, що циркулює в автоматизованих системах.

Перехоплення електромагнітних випромінювань базується на широкому використанні найрізноманітніших радіоприймальних засобів, засобів аналізу і реєстрації інформації, що має ряд наступних особливостей в порівнянні з іншими способами добування інформації: інформація видобувається без безпосереднього контакту з джерелом, на прийом сигналів не впливають ні час року, ні час доби, інформація виходить в реальному масштабі часу, в момент її передачі та випромінювання тощо.

В доповіді викладено результати досліджень побічних електромагнітних випромінювань інтерфейсу USB 2.0[2], виконаних для вирішення задач оцінки захищеності інформації на об'єктах інформаційної діяльності.

Структурна схема експериментальної установки наведена на рисунку 1.



1 – системний блок; 3 – принтер; 5 –аналізатор спектру.

2 – монітор; 4 – вимірювальна антена;

Рис. 1. Структурна схема експериментальної установки

Дослідження проводились за допомогою аналізатора спектру ROHDE&SCHWARZ FSW 13 (Signal&Spectrum Analyzer) з використанням антени R&S Active Dipole Antenna HE527 та USB флеш накопичувача Transcend J32 2GB.

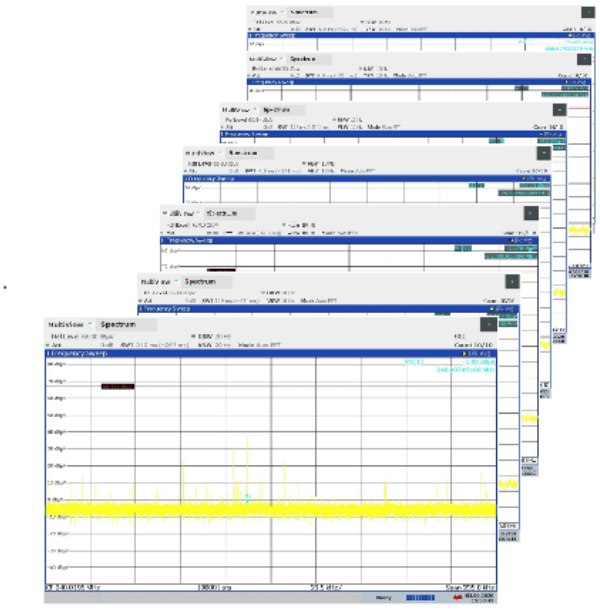


Рис. 2. Фотографії спектрограм сигналів інтерфейсу USB 2.0 при дослідженні побічних електромагнітних випромінювань

У результаті аналізу форми і спектра сигналів у кабелі USB (тестовий режим вимкнено, тестовий режим увімкнено) (рис.2) встановлено, що в USB- інтерфейсі постійно відбувається передача службових пакетів для

підтримки інтерфейсу. Під час увімкнення тестового режиму на спектрограмі з'являються додаткові послідовності імпульсів. Частота першої гармоніки для інтерфейсу USB 2.0 перебуває в околі 240 МГц.

Література

1. Про критичну інфраструктуру та її захист. Проект закону України від 27.05.2019 №10328. [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/JH7YW00A.html(дата звернення: 4.03.2021).

2. Яшкардин Владимир. USB. Universal Serial Bus Specification. Универсальная последовательная шина [Электронний ресурс] – Режим доступу:http://softelectro.ru/interface.html(дата звернення: 4.03.2021).

У*ДК 004.056*

Легомінова С.В.
доктор економічних наук, професор,
Державний університет телекомунікацій

АСПЕКТИ КІБЕРСТІЙКІСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ПРИКЛАДІ США

Провідні країни світу пріоритетним напрямом забезпечення інформаційної безпеки, як певного сегменту національної безпеки, визначають кіберстійкість об'єктів критичної інфраструктури. Дефініція "критична інфраструктура" в відповідності до змін зовнішнього середовища має перманентний характер до доповнень.

У 2018 р. Конгресом США було розроблено законопроект [1], яким запропоновано внести зміни у визначення дефініції "критична інфраструктура", що раніше було введено законом США (USA PATRIOT ACT, 2001) [2]. Зокрема, пропонувалося таке визначення: "Критична інфраструктура означає системи та ресурси, фізичні або віртуальні, що є надзвичайно важливими для Сполучених Штатів, а недієздатність або знищення таких систем та активів матиме катастрофічний регіональний чи національний вплив на здоров'я населення або безпеку, економічну безпеку або національну безпеку, в т. ч. *бази даних для реєстрації виборців, машини для голосування та інші системи зв'язку, які керують виборчим процесом, а також представляють і публікують результати від імені державних та місцевих органів влади.* (доповнення виділено курсивом.)".

Кіберстійкість критичних інфраструктур відносно новий термін, який з'явився з входженням цифровізації до всіх сфер нашого життя, особливо при впровадженні цифрових інструментів до економіки, що відразу викликало необхідність захисту певних сфер та бізнес процесів.

Основні стратегічні цілі ЄС та НАТО щодо кіберстійкості закріплено у Глобальній стратегії ЄС із зовнішньої політики та політики безпеки [3], та НАТО затвердило завдання щодо забезпечення національної кіберстійкості [4].

Міністерство внутрішньої безпеки США (МВБ; U.S. Department of Homeland Security, DHS) визначає дефініцію "стійкість" як "спроможність адаптуватися до змінних умов та протистояти загрозам порушень функціонування та швидко відновлюватися від порушень внаслідок криз" [5].

Відповідно до цього визначення формується завдання щодо забезпечення захисту критичної інфраструктури [6]:

- стійкість критичної інфраструктури – "спроможність підготуватись та адаптуватися до змінних умов, а також протистояти загрозам порушень функціонування та швидко відновлюватися від порушень. Стійкість включає спроможність протистояти загрозам та відновлюватися від цілеспрямованих атак, аварій, природних загроз та інцидентів";
- забезпечення безпеки критичної інфраструктури – "зменшення ризику критичної інфраструктури від втручання, атак або ефектів, спричинених природними катастрофами або людською діяльністю, за рахунок реалізації заходів із фізичного захисту або кіберзахисту".

Основними принципами успішного функціонування критичної інфраструктури визначено [7]:

- ініціативність і вирішення проблем безпеки;
- вчасне прийняття рішень з питань безпеки;
- застосування різноманітних кіберзасобів;
- організаційна готовність і вирішення бізнес-проблем;
- технічна гнучкість і адаптивність;
- ситуаційна обізнаність.

Управління кіберстійкістю об'єктами критичної інфраструктури маємо поділити на певні функціональні складові: управління, стратегія прав доступу користувачів, сегментування, активне реагування, забезпечення цілісності даних, моніторинг, методи відновлення і скоординований захист.

Отже, забезпечення кіберстійкісті об'єктів критичної інфраструктури передбачає можливість захисту від кіберзагроз за рахунок перманентних змін у нормативних документах, посиленні технологічних можливостей, які спроможні нівелювати загрози та зміцнити кіберстійкість важливої інфраструктури, телекомунікаційних мереж та послуг, випередити здійснення кіберзлочину та запровадженні функціонального управління.

Література

1. Defending American Security from Kremlin Aggression Act of 2018. URL: https://www. congress.gov/bill/115th-congress/senate-bill/3336/text?q=%7B%22search%22%3A%5B% 22S.3336%22%5D%7D&r=1.

2. Закон США (USA PATRIOT ACT, 2001). URL: https://www.congress.gov/bill/107thcongress/house-bill/3162.

3. A Global Strategy for the European Union's Foreign And Security Policy. URL: https://eeas. europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.
4. Commitment to enhance resilience. URL: http://www.nato.int/cps/en/natohq/official_ texts_133180.htm?selectedLocale=en.
5. Department of Homeland Security. Resilience. URL: https://www.dhs.gov/topic/resilience.
6. Presidential Policy Directive – Critical Infrastructure Security and Resilience. (2013). URL: https://www.dhs.gov/sites/default/files/publications/PPD-21-Critical-Infrastructure-andResilience-508.pdf.
7. Cyber Resilience: Part Three What is Cyber Resilience? URL: https://blog.blackswansecurity.com/ 2016/02/part-three-what-is-cyber-resilience.

УДК 343.102: 343.17

Метелев О.П.
Інститут підготовки юридичних кадрів для СБУ
Національного юридичного університету ім. Я. Мудрого

ІНФОРМАЦІЙНИЙ ПРОСТІР ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПРОБЛЕМА ВИЗНАЧЕННЯ ЮРИСДИКЦІЇ

У сучасному світі глобальний інформаційний простір, який являє собою єдність двох складових: технічної (глобальна мережа Інтернет з телекомунікаційною інфраструктурою зв'язку і комунікаціями), а також соціальної (глобальна спільнота Інтернет-користувачів), став одним із ключових чинників, який суттєво впливає на стан і розвиток інформаційної безпеки та має необмежений потенціал для економічного і соціального розвитку держави. Однак, разом з перевагами розвиток цифрових технологій і телекомунікацій привніс низку суттєвих проблемних питань, які обумовлені вразливістю кіберпростору щодо несанкціонованого стороннього втручання та модифікації цифрової інформації.

Водночас, законодавець на сьогодні не дає чіткого нормативного визначення поняття «інформаційний простір». В нормативно-правових актах вітчизняного законодавства (загалом їх біля 20) лише вказується на «інформаційний простір», але не розкриваються його природа та істотні ознаки. Так, в п. 8 ч. 1 ст. 3 Закону України «Про інформацію» лише вказується, що «одним з основних напрямів державної політики є сприяння міжнародній співпраці в інформаційній сфері та входження України до світового інформаційного простору» [1]. В п. 2 ст. 12 Закону України «Про засади внутрішньої та зовнішньої політики» говориться, що «основними засадами зовнішньої політики є: … підтримка інтеграції України у світовий інформаційний простір» [2]. В свою чергу, ст. 2 Доктрини інформаційної безпеки України встановлює, що основною метою реалізації положень Доктрини є

«створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету» [3].

З огляду на нормативну невизначеність цього поняття, науковці в своїх дослідженнях намагались надати своє тлумачення «інформаційного простору».

Можливо погодитись з думкою О.М. Селезньової, яка зазначила, що «інформаційний простір – це частина інформаційної сфери, обмеженої матеріальною та нематеріальною територією поширення, центром якої є сукупність суб'єктів, що здійснюють інформаційну діяльність, а її складовими – інформація та інформаційні відносини, інформаційна наука та інформаційна культура, інформаційна діяльність та інформаційна інфраструктура, інформаційне право та інформаційне законодавство. беручи до уваги значення для України [4, с. 136].

Екстериторіальність – є характерною ознакою інформаційного простору. Дана обставина ставить під сумнів традиційне поняття територіальної юрисдикції, а також основні норми міжнародного права в частині, що стосуються визначення місця злочину в інформаційному (кібернетичному) просторі.

На сьогодні науковці, зазвичай, під місцем злочину, в узькому сенсі, вважають територію, де безпосередньо було скоєне протиправне діяння і на якій можливо передбачити зміни в оточуючому середовищі, обумовлені цим явищем. В широку сенсі, місце злочину – це шляхи підходу і втечі з місця події, а також прилягаючі ділянки. Такі ознаки як безпосередність, наявність змін в оточуючому середовищі, не підпадають під визначення інформаційного простору, який створений і існує як екстериторіальне штучне утворення. При цьому у кримінальному законодавстві не існує такого поняття, як злочин, скоєний в інформаційному просторі, однак, в деяких статтях Кримінального кодексу України глобальна мережа Інтернет (окремий випадок інформаційного простору) виділяється як кваліфікуюча ознака, але залишається відкритим питання щодо конкретизації місця злочину в кіберпросторі.

Таким чином, можливо запропонувати вважати «місцем вчинення злочину» передбачену диспозицією кримінально-правової норми ознаку об'єктивної сторони складу злочину, яка характеризує певну територію, інше місце, у тому числі частину інформаційного простору (сайт, домен), які характеризуються фізичними, соціальними і правовими критеріями, де суб'єкт вчинив передбачену кримінальним законом дію або бездіяльність.

Законодавче визначення «місця вчинення злочину» дозволить, по-перше, визначити юрисдикцію судів стосовно злочинів скоєних в інформаційному (кібернетичному) просторі, описати конкретні владні повноваження суду під час здійснення правосуддя і судового контролю у кримінальних

провадженнях, а по-друге удосконалити визначення підслідності кримінальних правопорушень скоєних в кіберпросторі або з використанням цифрових технічних засобів, що напряму впливатиме на швидкість та якість проведення досудового розслідування.

Література

1. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 07.03.2021).

2. Про засади внутрішньої та зовнішньої політики: Закон України від 01 липня 2010 року № 2411-VI. URL: https://zakon.rada.gov.ua/laws/show/2411-17 (дата звернення: 07.03.2021).

3. Доктрина інформаційної безпеки: Затверджено Указом Президента України від 25 лютого 2017 року № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017 (дата звернення: 07.03.2021).

4. Селезньова О.М. Теоретико-методологічне трактування окремих засадничих категорій інформаційного права. *Вісник Асоціації докторів філософії України*. *Спецвипуск «ІТ право»*. Львів, 2016. С. 136-142.

УДК 355.40:356.35

Мілих Є.Г.
Національний університет оборони України
імені Івана Черняховського

МЕТОДИКА ОЦІНЮВАННЯ ЗАХОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Виходячи з того, що які кошти країна може виділити на захист національної інфраструктури, національне законодавство повинно встановити критерії віднесення тих чи інших об'єктів та систем до критичної інфраструктури, спираючись на затверджені методи оцінки загроз та ризиків сталому її функціонуванню. Такі переліки використовуються при плануванні відповідних заходів та у процесі прийняття рішень. Вони, як правило, підлягають перегляду, періодичному або при значних змінах у безпековому середовищі та при внесенні істотних змін у національне законодавство тощо.

Заслуговує на увагу визначення критичності, наведене у Національній стратегії захисту критичної інфраструктури: критичність – це відносна міра важливості даної інфраструктури, що враховує вплив раптового припинення її функціонування, або функціонального збою на безпеку постачання, тобто забезпечення суспільства важливими товарами і послугами.

Комплексне дослідження існуючих складових інформаційної безпеки держави у воєнній сфері [1; 2] показало, що існуючі підходи до визначення

переліку елементів критичної інфраструктури (віднесення об'єктів до критичної інфраструктури) засвідчує, що можуть враховуватися, зокрема, такі характеристики:

масштаб (географічне охоплення території, для якої втрата елементу критичної інфраструктури викликає значну шкоду);

вразливість об'єкту до впливу небезпечних чинників;

безпека життєдіяльності та здоров'я населення (число постраждалих, загиблих, осіб, які отримали серйозні травми, а також чисельність евакуйованого населення, забезпечення роботи аварійно-рятувальних служб, екстреної допомоги населенню);

екологічна безпека (вплив на навколишнє природне середовище).

Тому метою тез доповіді є опис методики оцінювання заходів забезпечення безпеки об'єктів критичної інформаційної інфраструктури.

Деталізація показників, за якими визначається важкість наслідків, значною мірою залежить від сектору критичної інфраструктури.

Процес ідентифікації елементів критичної інфраструктури має включати аналіз взаємозв'язків між елементами критичної інфраструктури та оцінені наслідки можливого припинення їх функціонування (аварії тощо) на довготривалий період [3].

Після визначення категорій та ідентифікації об'єктів критичної інформаційної інфраструктури необхідно визначитися з поняттям захисту критичної інфраструктури. Захист критичної інфраструктури України – це комплекс заходів, реалізований в нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури.

Методика оцінювання заходів забезпечення безпеки об'єктів критичної інформаційної інфраструктури розглядається на моделі процесу функціонування складної системи, яка має наступні етапи:

визначення вихідних даних;

знаходження мінімуму цільової функції часу;

знаходження точок безумовного мінімуму функціонування системи;

обчислення оптимального значення середнього часу заходів забезпечення безпеки об'єкту;

аналіз отриманих результатів.

Відповідно до цієї моделі, формула 1 визначимо залежність середнього часу обслуговування замовлень від інтенсивності надходження замовлень на вибірку даних з локальних вузлів.

Таким чином, завдання визначення оптимального значення коефіцієнту інформаційної загрози об'єкту критичної інформаційної інфраструктури Kr для військових об'єктів критичної інформаційної інфраструктури зводиться до задачі пошуку мінімального аргументу середнього часу обслуговування замовлень і представлена наступною цільової функцією:

$$Kr = \arg\min\left(\overline{T}\left(\lambda_{qr}, \lambda_{ur}\right)\right) \qquad (1)$$

Проте розв'язання отриманої системи рівнянь аналітично зв'язано з пошуком коренів шостого порядку. Ступінь з'являється під час приведення елементів рівнянь до загального знаменника. У зв'язку з цим для розв'язання необхідно використовувати чисельні методи розв'язання нелінійних задач з лінійними обмеженнями [4].

У загальному вигляді вирішення задачі знаходження мінімуму середнього часу впливу інформаційної загрози на об'єкт критичної інформаційної інфраструктури здійснюється за декілька етапів може бути реалізовано в межах методу лінійних комбінацій, в основі якого лежить градієнтний метод найшвидшого спуску модифікований для застосування при наявності лінійних обмежень.

Таким чином, однією із властивостей критичної інфраструктури відноситься її стійкість до впливу негативних чинників. Під стійкістю критичної інфраструктури розуміємо її здатність надійно функціонувати у нормальному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після аварій та технічних збоїв, зловмисних дій, природних лих та небезпечних природних явищ.

Література

1. Словник основних термінів у галузі інформаційної безпеки держави у воєнній сфері. – К.: НУОУ, 2014.

2. Cornish Paul, Lindley-French Julian, Yorke A.Claire. Strategic communications and National Strategy. London. Chatham House Report (The Royal Institute of International Affairs). 2011. September.

3. Dennis M.Murphy. Strategic Communication Talking the Talk: Why Warfighters Don't Understand Information Operations / Center for Strategic Leadership; U.S. Army War College. 2009. May. Volume 4-09.

4. Development, Concepts and Doctrine Centre, Joint Doctrine Note 1/11, 'Strategic Communication: The Defence Contribution'. 2011. March. (Shrivenham: DCDC).

УДК 004.054

Моклякова К.П.
Бабенко Т.В.
доктор технічних наук, професор
Бігдан А.М.
Ігніска В.І.
Київський національний університет імені Тараса Шевченка

МОДЕЛІ ОЦІНЮВАННЯ ПРОФЕСІЙНИХ КОМПЕТЕНЦІЙ АУДИТОРІВ

Аудитор інформаційної безпеки (аудитор ІБ) – професія, що передбачає неупереджену оцінку ефективності використання методів захисту інфо-

рмації. Відповідальність за визначення вимог до знань, сертифікацію аудиторів ІБ покладається на Державну службу спеціального зв'язку та захисту інформації України, згідно Положення КМУ [1]. Однак, існує певна невизначеність щодо методології оцінки професійних компетенцій аудиторів ІБ в Україні [2].

Методи оцінки компетенцій описані в ISO 19011. Критерії оцінювання включають: освітній рівень, досвід роботи в галузі ІБ, професійну кваліфікацію, результати співбесіди і т.д. Ці методи мають різні показники якості: деякі можна представити у вигляді двійкових змінних, а інші - ні.

При прийомі на роботу працівника, організація проходить етапи: підбору і відбору [3]. Для аудиту ІБ об'єктів критичної інфраструктури, на етапі відбору визначають критерії: необхідність допуску кандидата до інформації з обмеженим доступом, досвід роботи, освітній рівень, наявність сертифікатів. Етап відбору поділяється на: аналіз заяв та наданої кандидатами інформації; проведення співбесід та тестування. При аналізі заявок, аудитори, які не відповідають сформованим раніше вимогам, будуть відсіяні. Співбесіди та тестування спрямовані на оцінку професійних компетенцій аудитора ІБ.

Тестування – об'єктивна оцінка кваліфікації аудитора. Для авторитетності тесту, необхідно створення національної сертифікації аудиторів ІБ. Тест повинен складатися з бази запитань, за підходами організації ISACA, сімейства стандартів ISO 27000, PCI DSS та ін.

Використання моделі Раша [4] для оцінки здібностей надає достовірні результати, шляхом використання статистики адекватності та карти кореляції рівня складності завдань з рівнем компетенцій особи. Вимоги до питань згідно моделі Раша: міра рівня підготовки кандидата $t_i \in (0; \infty)$; імовірність правильної відповіді P_i- залежить від підготовки фахівця та рівня складності завдання $b(0; \infty)$, або $P = f(t, b)$.

Для побудови шкали вимірювань, зображаємо рівень готовності t та рівень складності b на логарифмічній шкалі: $\theta = \ln(t)$, $\beta = \ln(b)$, де θ і β значення рівнів готовності та складності, виміряні за логарифмічною шкалою (логіти). Функція ймовірності "перемоги" випробуваного при відповіді на питання (1)

$$P_j(\theta) = \{x_{ij} = 1 \,|\beta_j\} = \exp\frac{\theta-\beta_j}{1+\exp(\theta-\beta_j)} \quad (1)$$

Розподіл співвідношення логітів готовності та складності одного питання повинен зростати логарифмічно. Адекватність запитань визначається ступенем відхилення емпіричних точок від характерної кривої.

Окрім тестування, є інші фактори оцінки аудитора ІБ. Модель підбору повинна містити велику кількість показників з ендогенними параметрами (мають значення 0/1), тому використовуємо бінарну модель вибору з функцією логістичного розподілу.

Змінна Y - можливість або неможливість зайняти посаду аудитора ІБ, має 2 значення $y = \{0;\ 1\}$. Імовірність того, що вона прийме одне зі значень - функція декількох факторів $x^T = \{x_1, x_2, \dots x_i\}$ (2), (3):

$P(Y = 1|x) = F(x^T\beta)$ (2) $\quad P(Y = 0|x) = 1 - F(x^T\beta)$ (3)

Набір параметрів β - вплив змін кожного фактора на кінцеву ймовірність. Необхідно знайти адекватну функцію в правій частині рівняння. Логітна модель двійкового пошуку використовує функцію логістичного розподілу (4):

$$P(Y = y|x) = \exp(x^T\beta)\,/(1 + \exp(x^T\beta)) = \Lambda(x^T\beta) \quad (4)$$

Після всіх перетворень маємо рівняння правдоподібності (5):

$$\frac{dLnL}{d\beta} = \sum_{i=1}^{n}[\frac{y_i f_i}{F_i} + (1 - y_i)\frac{-f_i}{(1-F_i)}]x_i = 0. \quad (5)$$

Для вирішення рівняння використовується багатовимірна інтерпретація методу Ньютона, де L - функція Лагранжа, H - матриця Гесса (6):

$$\beta^{j+1} = \beta^j - H^{-1}(\beta^j)gradL(\beta^j) \quad (6)$$

Використання бінарної регресії для оцінки кандидата засноване на необхідності кількісної інтерпретації якісних змінних (досвід аудиту включає оцінку організацій, де він проводився).

У процесі класифікації вибірці присвоюється опис атрибута - вектор, компонентами якого є різні кількісні та якісні характеристики. Завдання алгоритму класифікації - присвоєння об’єкта до класу.

Для обрахунку результату використовуємо штучні нейронні мережі. Мережа є системою взаємопов’язаних нейронів, які апроксимують функції для побудови розподільної поверхні великої складності й ефективної класифікації.

Застосовуючи різні моделі, можна визначити автоматизований процес найму аудиторів ІБ. Отже, необхідні подальші дослідження для створення бази питань та навчання штучної нейронної мережі для досягнення комбінованої моделі оцінки професійних компетенцій аудиторів ІБ.

Література

1. КМУ «Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України», 2006.

2. K.MOKLIAKOVA, A.BIGDAN, T.BABENKO Information security auditors’ professional competencies assessment models, 2020.

3. ZINCHENKO A. A., Modeling of processes of selection and assessment of personnel, 2016.

4. DEMENCHENKO O.G. Mathematical foundations of Rasch Measurement, 2010.

УДК 004.056.53
Мужанова Т.М.
кандидат наук з державного управління, доцент,
Державний університет телекомунікацій

ІНДИКАТОРИ ІНСАЙДЕРІВ ВІДПОВІДНО ДО КОНЦЕПЦІЇ CERT

Як свідчить статистика, шкідливий інсайд є однією з найбільш серйозних і широко поширених загроз для інформаційної безпеки організації, зокрема у 2019 році 34% випадків порушень, пов'язаних з даними, сталися із залученням інсайдерів [1], а при здійсненні більше 50% успішних хакерських атак на корпоративні ІТКС хакери мали спільників серед персоналу компанії-жертви.

Саме тому запобігання та протидія внутрішнім загрозам є важливим і обов'язковим напрямом забезпечення інформаційної безпеки організації. Особливого значення така діяльність набуває у забезпеченні інформаційної та кібербезпеки об'єктів критичної інфраструктури держави, оскільки порушення систем захисту ІТКС загальнодержавного рівня можуть мати масштабні наслідки і завдати значної шкоди національним інтересам.

Для ефективного забезпечення інформаційної безпеки необхідним є запобігання внутрішнім загрозам, а кожна компанія має докласти максимум зусиль для того, щоб виявити інсайдера до здійснення ним деструктивних дій. На думку фахівців CERT, є кілька категорій індикаторів, які можуть свідчити про шкідливу інсайдерську діяльність: особисті, поведінкові, біографічні й технологічні (діяльності в мережі, клієнтських дій та використання сервісів), і допомогти виявити внутрішнього порушника [2].

Особисті індикатори (Personal Indicators). Часто причинами інсайдерських інцидентів є проблеми в особистому житті порушників, які підштовхують їх до вчинення різного роду зловмисних дій з метою отримати фінансову вигоду (крадіжки, шахрайство та шпигунство). До особистих показників потенційної інсайдерської діяльності відносять наявність у працівника депресії або інших негативних емоційних станів, які викликані зміною місця проживання, втратою близьких родичів або друзів, розривом стосунків з коханою людиною або розлученням тощо. Крім того, такими чинниками можуть бути надмірні фінансові зобов'язання або втрата джерел доходу, звільнення з місця роботи.

Поведінкові індикатори (Behaviour Indicators) Другою групою показників, які можуть бути встановлені тільки впродовж певного часу та сигналізувати про наявність потенційного зловмисного інсайдера в компанії, є показники, що характеризують поведінку персоналу. Серед них, зокрема, небажання працівника дотримуватися встановлених правил і процедур ін-

формаційної безпеки, здійснення повторних порушень, надмірне або невиправдане використання копіювального обладнання, надання допомоги співробітникам, що має наслідком доступ до конфіденційних даних, зайва понаднормова робота. Крім того, прояви недбалості, агресії, імпульсивність у поведінці та погані відносини з колегами також можуть опосередковано свідчити про приховані деструктивні дії працівника.

Біографічні індикатори (Background Indicators). На відміну від попередніх індикаторів, які базувалися на суб'єктивних оцінках працівника, показники попереднього досвіду є результатом об'єктивної перевірки біографічних даних особи. Така перевірка має на меті встановлення фактів з минулого особи, що можуть відчити про її злочинні схильності: взаємодія з особами або групами, які просувають ідеї, спрямовані проти організації, наявність судимості, фінансових заборгованостей, залежності (алкоголь, наркотики, азартні ігри), психічних або емоційних розладів. Про ненадійність працівника говорить факт частої зміни попередніх місць роботи і коротка їх тривалість, а також життя «на широку ногу», коли витрати перевищують дохід.

Індикатори використання комп'ютерних мереж (Computer Networks Indicators). Важливе значення для виявлення внутрішніх порушників має моніторинг мережі, в результаті якого можуть бути встановлені факти підозрілої діяльності персоналу, зокрема переписки з конкурентами, надсилання е-листів з аномально великим обсягом даних, DNS-запити, які вказують на роботу з ресурсами тіньового Інтернету, використання підозрілих протоколів (наприклад, IRC) та сервісів (наприклад, VPN, Tor), неправомірних технологічних засобів, шкідливих програм, підключення до мережі несанкціонованих пристроїв тощо.

Індикатори клієнтської діяльності (Client-side Indicators), тобто дій, які відбуваються на клієнтській частині моделі «клієнт-сервер», також дають можливість виявити шкідливого інсайдера. Так, встановлення фактів зберігання заборонених файлів, спроб відключення антивірусних засобів або під'єднання невідомих пристроїв (USB, CD-ROM), невдалих спроб авторизації, намагань перевищити права доступу до інформації або копіювати конфіденційні документи, ввійти в систему в неробочий час, а також відсутність даних реєстрації подій або моніторингу є підставою для проведення ґрунтовної перевірки підозрілої особи.

Індикаторами використання сервісів (Service Indicators) є випадки модифікації централізованих реєстраційних файлів, копіювання великого числа документів на локальний диск, невдалі спроби автентифікації, внесення змін у файл конфігурації, дозволи та бази даних, отримання доступу до ресурсів, непов'язаних з повноваженнями користувача, використання одного

облікового запису користувача з різних пристроїв, наявність кількох облікових записів в одного користувача, встановлення терміну дії облікового запису до 30-ти днів.

Отже, для виявлення потенційних внутрішніх порушників інформаційної безпеки організації доцільно використовувати методику CERT, яка передбачає моніторинг і аналіз особистих, поведінкових, біографічних і технологічних індикаторів підозрілої діяльності персоналу.

Література

1. Data Breach Investigations Report – 2020. Learn to protect your organization from cyberthreats. URL: https://enterprise.verizon.com/resources/ reports/dbir/ (дата звернення: 09.03.2021).

2. Kont M., Pihelgas M., Wojtkowiak J., Trinberg L., Osula A. Insider Threat Detection Study : Publication of the NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf (дата звернення: 09.03.2021).

УДК 341.238 (477) (045)

Ожеван М.А.
доктор філософських наук, професор,
Національний інститут стратегічних досліджень

ГЕОПОЛІТИЧНІ ВИКЛИКИ ГЛОБАЛЬНИХ ІНФОДЕМІЧНИХ ВІЙН

Загальновизнаним у науковому співтоваристві є той факт, що питання подолання коронавірусної пандемії є не тільки питанням медико-епідеміологічним, але й політичним та геополітичним, питанням великої інформаційної «гри».

Звичайно, у подібному геополітичному прогнозуванні постпандемічного світоустрою є чимало необґрунтованого мрійництва і конспірології, хоча є й достатньо елементів раціонально обґрунтованого алармізму. Зокрема такий поважний політичний мислитель як Джозеф Най-молодший (один із авторів концепту «м'якої сили») попереджає щодо обумовленої пандемією небезпеку «авторитарного виклику», подібного до того, який призвів до падіння демократії у більшості європейських країн у 1930-ті роки та щодо ймовірності наближення «прокитайського світового порядку» (англ. «A China-dominated world order») [1].

У свою чергу, «Бюлетень американських науковців-атомників», який провадить моніторинг дезінформації, дедалі частіше присвячує свої матеріали з даної тематики «коронавірусній дезінформації», яку використовують

правителі авторитарної Росії та комуністичного Китаю з метою переформатування світової геополітики. Одним із засобів подібного переформатування засобами дезінформації є різноманітні «фундації», які мають свої Інтернет-представництва і які залучають для більшої переконливості своїх матеріалів маргінальних науковців-політологів або квазінауковців з явно вираженим хистом до конспірології [2]. Прикладом може бути «Фундація стратегічної культури» («The Strategic Culture Foundation») [3]. Відповідно до Доповіді «Центру глобального залучення» Державного департаменту США, оприлюдненій у серпні 2020 р., згаданий російський thank tank безпосередньо пов'язаний з російською спецслужбою ФСБ, а опосередковано - з розвідувальним підрозділом Міністерства закордонних справ РФ (МИД РФ) [4].

Відомо, що «світовий порядок», який спроможні забезпечити великі державні або наддержавні утворення («імперії») прийнято позначати латинським терміном «Pax», який має подвійне смислове навантаження, означаючи і «наддержаву» і «мир» у розумінні «світового порядку». Йдеться наприклад про «Pax Romana» або «Seculum Romano» («Римський Світ (Мир)»; «Римські століття»), що потривав два століття (від 20 р. до н.е. – до 180 р. н.е.). Звичайно, цей світоустрій не означав «суцільного миру». Хоча в умовному центрі Імперії (метрополії) дійсно панував мир, але на її периферії (у колоніях) точилися невпинні війни. Щодо руйнації «Pax Romana», то її істотно пришвидшила, на думку істориків, пандемія, відома під такими історичними назвами як «чума Галена» або «Антонінова чума» (165-180 рр.).

«Британське століття» («Pax Britannica»; англ. «The British Century») (1815-1918 рр.), у свою чергу, зруйнувала не тільки Перша Світова війна, але й епідемія вельми летального грипу, відомого як «іспанка», яка забрала біля 50 млн. людських життів, тобто втричі більше ніж сама війна (17 млн.).

«The American Century» або «Pax Americana», розпочавшись після закінчення Другої Світової війни, станом на 2020 р. триває уже 75-ть років. «Pax Americana» остаточно утвердився після краху в 1991 р. СРСР. Однак й досі невідомо, чи буде друга половина XXI століття також «американською».

«Pax Russica» та його історичний аналог «Pax Sovietica» («Російський Світ (Мир)»; «Радянський Світ (Мир»), - терміни, які були особливо актуальними у період «Холодної війни» й біполярного світу, коли Росія (СРСР) була другим полюсом сили у світовій геополітичній змагальності. Звичайно, сучасній путінській Росії важко розраховувати на поновлення своєї імперської величі. Разом з тим сакраментальна теза Володимира Путіна, висловлена ним у 2005 році у традиційному Посланні Федеральним Зборам РФ про те, що крах СРСР був найбільшою геополітичною катастрофою XX століття засвідчила, що принаймні на рівні політичної риторики та «гри у дезінформацію» путінська Росія не проти включитися у геополітичне протиборство [5]. У тій же великодержавній тональності Володимир Путін у травні 2014 р. за-

явив: «Модель монополярного світу є помилковою…Світ є мультиполярним». Варто зазначити, що безпосереднім приводом для подібної путінської заяви були санкції, накладені на Росію у зв'язку з російською «гібридною» агресією проти України (зокрема – анексією Криму) [6].

Звичайно, Росія не розраховує у подібному протиборстві на власні цілковито обмежені економічні та фінансові ресурси (за номінальним ВВП – Росія тільки 11-та економіка світу, цілковито співставна з економіками Італії або Південної Кореї), а на ресурси свого великого сусіда – КНР й примарні перспективи утворення «Pax Sinica» («Китайського Світу (Миру)» або ж його промосковської версії - «Pax RussoSinica».

Отже, одним із чинників, які підточують очолюваний США світовий порядок, стала коронавірусна пандемія, одним малоприємних наслідків якої є непопулярні практики обмеження різноманітних прав і свобод людини включно зі свободами слова й міжлюдських контактів з метою виграти час у боротьбі з пандемією, протидіяти панічним настроям серед населення тощо. Критики західного способу життя та очолюваного США світового порядку звертають передусім увагу на те, що у боротьбі з пандемією США, Великобританія та країни ЄС демонструють наразі буцімто неадекватний рівень керівництва та суспільної згуртованості, чого не можна сказати про країни Азійсько-Тихоокеанського регіону. Відтак, робляться висновки щодо посилення геополітичних позицій Китаю, що може посприяти посиленню агресивності Росії й навіть утворенню китайсько-російського воєнно-політичного союзу, про який заявляв у виступі на Валдайському Дискусійному Форумі 2020 року Володимир Путін [7].

Література

1. Joseph S. Nye. Geopolitics after the pandemic // The Strategist (The Australian Strategic Policy Institute - ASPI). 7 Oct 2020. - ttps://www.aspistrategist.org.au/geopolitics-after-the-pandemic/.
2. Isra Thange, Nicola Bariletto, Luca Zanotti, Jacob Rob, Samikshya Siwakoti, Jacob N. Shapiro. How Russia, China, and other governments use coronavirus disinformation to reshape geopolitics // The Bulletin of the Atomic Scientists. October 12, 2020. - https://thebulletin.org/2020/10/how-russia-china-and-other-governments-use-coronavirus-disinformation-to-reshape-geopolitics.
3. The Strategic Culture Foundation. - https://www.strategic-culture.org/.
4. Global Engagement Center (GEC) Special Report: August 2020. Pillars of Russia's Disinformation and Propaganda Ecosystem. - https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf/.
5. Владимир Путин: "Распад СССР - крупнейшая геополитическая катастрофа века" // ИА REGNUM. https://regnum.ru/news/polit/444083.html.

6. Vladimir Putin Warns Sanctions on Russia Will Back on West // Telegraph, May 23, 2014. - http://www.telegraph.co.uk/news/worldnews/europe/russia/10851908/Vladimir-Putin-warns-sanctions-on-Russia-will-backªre-on-West.html.

7. Путин допустил возможность военного союза России и Китая // РБК. 22 октября 2020 г. - https://www.rbc.ru/rbcfreenews/5f91c7c49a7947ee9e93d378.

УДК 355.40:356.35

Порохня І.М.
Рахімов В.В.
Національний університету оборони України
імені Івана Черняховського

АНАЛІЗ ВИКОРИСТАННЯ ГЛОБАЛЬНИХ КІБЕРМЕРЕЖ ДЛЯ ВИКРАДЕННЯ ІНФОРМАЦІЇ

В даний момент ІТС ЗС України надає всі послуги для обміну інформацією в внутрішній мережі. Проте особливості побудови ІТС відкривають для зловмисників ряд вразливостей за допомогою яких чутлива інформація може потрапити до них. Можемо виділити такі аспекти, а точніше пробіли в безпеці важливої інформації:

1. Створення та використання папок у відкритому доступі, а також використання власних FTP серверів. Використання таких папок у військових організаціях дах широкий функціонал для користувачів (обмін файлами, синхронне редагування, зберігання інформації в зручному та постійно доступному місці), та одночасно несе за собою можливість доступу до цієї інформації зловмисників, які засобами моніторингу виявляють такі папки (сервери) у відкритому доступі та завантажують у свої колекції гігабайти службової інформації.

2. Використання пристроїв у мережевому доступі (принтерів, сканерів, плотерів), несе за собою можливість зловмисників до викрадення інформації, яку відправляють на друк чи сканування.

3. Для контролю за обміном повідомленнями та документами в ЗС України розгорнуто поштові сервери та систему електронного документообігу. Дані сервіси контролюється підрозділами по забезпеченню кібернетичної безпеки, тобто виток інформації з такого серверу чи системи зведений до мінімуму. Проте користувачам не завжди до вподоби використання даних сервісів і вони наполегливо користуються сторонніми поштовиками та файловими обмінниками. Результатом цього є втрата гігабайтів інформації, що були передані таким способом.

Викрадення та аналіз такої інформації здійснюється зловмисниками з метою отримання розвід-даних, а в деяких випадках така інформація використовується, для публікації в ЗМІ, з метою компрометації Збройних Сил України, дестабілізації ситуації в підрозділах та є доказом безвідповідальності користувачів ІТС ЗС України.

Варто зауважити, що ІТС ЗС України функціонують та виконують завдання за призначенням, проте через безвідповідальність деяких користувачів, точками входу до ІТС може стати необачно підключений до АРМ пристрій для виходу в Інтернет.

Так для доступу в інтернет використовуються бездротові модеми, мобільні термінали з 3G передавачами, роутери з можливістю підключення до антен провайдерів, що в свою чергу спричиняє неконтрольований доступ до ІТС, з можливістю викрадення інформації та керування АРМ у мережі. Варто зауважити, що такі дії користувачів є протиправними.

В свою чергу існує багато інструментів та способів, за геопозиціями чи за особистими даними виявити таких користувачів, та отримати доступ до ІТС.

В рамках роботи висвітлимо один із таких інструментів. Онлайн скане Shodan.

Shodan –пошукова система, яка акумулює в собі всі підключення, облікові дані пристроїв, місцезнаходження, всі характеристики, точки входу. Однією з особливостей використання даної пошукової системи є те, що за геопозицією можна вирахувати користувача, що є на території де розгорнуто ІТС, та отримати інформацію для проведення кібернетичної атаки.

Отже, у сучасних умовах одною з головних складових є кібернетична безпека ІТС ЗС України. Питання кібернетичних загроз та кібернетичного захисту гостро стоїть у військовій сфері, з причини того, що управління військами, зв’язок, а також складова суспільної інформаційної боротьби стала невід’ємною складовою повсякденного життя ЗС України в умовах гібридної війни.

Визначення наявних загроз кібернетичній безпеці, є одним з початкових етапів на шляху створення та вдосконалення наявної системи забезпечення кібернетичної безпеки в ІТС ЗС України. В рамках написання цієї роботи було проведено аналіз сегменту кібернетичного впливу в ІТС ЗС України. Визначено, що основним сегментом ІТС ЗС України є ВЗ. Основними об’єктами захисту є: маршрутизатори, сервери, телекомунікаційне обладнання та користувачі ІТС. Розглянуто основні засоби для забезпечення кібернетичного захисту, та поняття кібернетичного захисту згідно наявного законодавства в галузі кібернетичної безпеки.

В ході проведення дослідження було встановлено, що основними типами кібернетичних загроз ІТС ЗС України є: атаки підготовчих періодів, високотехнологічні атаки, вірусні атаки (ШПЗ) та соціальна інженерія. Також було проведено аналіз наявних кібернетичних загроз та вразливостей

на сегмент ІТС ЗС України, зокрема вразливості телекомунікаційних систем, атаки типу інсайдерства, використання даних якими обмінюються в глобальній мережі інтернет, а також дослідили проблему підключення сторонніх пристроїв. В розрізі дослідження були проаналізовані можливі сценарії проведення кібернетичного впливу на ІТС ЗС України з можливістю використання виявлених загроз.

Таким чином, провівши дослідження можна зробити висновки, що використання глобальних кібермереж для викрадення інформації в може призвести до втрати важливої інформації, деструктивного впливу на систему зв'язку ЗС України, компрометації інформації, яка циркулює в ІТС ЗС України та деструктивному впливу на систему управління.

Література

1. Cornish Paul, Lindley-French Julian, Yorke A.Claire. Strategic communications and National Strategy. London. Chatham House Report (The Royal Institute of International Affairs). 2011. September.

2. Dennis M.Murphy. Strategic Communication Talking the Talk: Why Warfighters Don't Understand Information Operations / Center for Strategic Leadership; U.S. Army War College. 2009. May. Volume 4-09.

УДК 004.056

Савченко В.А.
доктор технічних наук, професор
Лаптєв О.А.
доктор технічних наук, старший науковий співробітник
Кітура О.В.
Державний університет телекомунікацій

ВИЯВЛЕННЯ ІНСАЙДЕРСЬКИХ ЗАГРОЗ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ЖУРНАЛІВ АКТИВНОСТІ КОРИСТУВАЧІВ

На сьогоднішній день основне джерело кібератак поступово зміщується від зловмисних аутсайдерів чи ботів до цілком довірених працівників організації, які мають доступ до важливої інформації та можуть вчиняти зловмисні дії умисно чи ненавмисно. За даними щорічного видання Insider Threat Report від компанії Cybersecurity Insiders у 2020 році 68 % опитуваних організацій визнали свою беззахисність до інсайдерських атак. При цьому 63 % очікують атак від привілейованих ІТ користувачів чи системних адміністраторів, 51 % вважають загрозою власних звичайних працівників, 50 % бачать загрозу з боку провайдерів та тимчасових працівників організації [1].

Сучасні методи виявлення інсайдерських загроз базуються на аналізі поведінки користувачів протягом деякого часу [2]. Зазначені методи вже реалізовані у багатьох системах: UEBA (User and Entity Behavior Analytics), DLP (Data Loss Prevention) та SIEM (Security Information and Event Management). Даними для аналізу такої поведінки є записи (logs) журналів активності, які дають змогу виявляти аномалії у різних сценаріях діяльності користувачів. Для аналізу застосовуються методи математичної статистики, Баєсівського оцінювання та інтелектуального аналізу даних (Data Mining). Проте, більш ефективним є пошук інсайдера за допомогою нейронних мереж, зокрема, на основі моделей глибокого переконання (DBN – Deep Belief Networks). Модель DBN складається з декількох шарів обмежених машин Больцмана (RBM – Restricted Boltzmann Machine) – стохастичних штучних мереж, здатних навчатися за розподілом ймовірностей (рис. 1) [3].

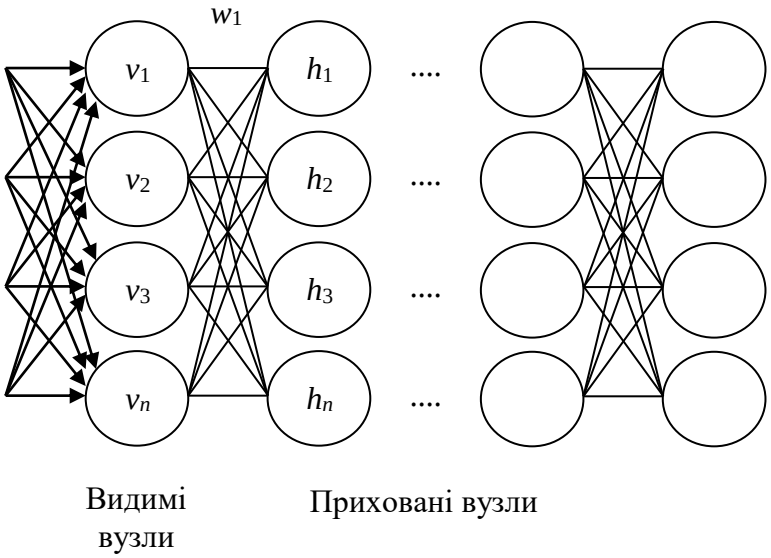


Рис. 1. Мережа глибокого переконання на основі обмежених машин Больцмана

Робота DBN полягає у переборі параметрів структури RBM, яка складається з видимого (v) та прихованого (h) шарів. Вузли одного шару між собою не з'єднані, тоді як вузли різних шарів з'єднані один з одним. При цьому розподіл ймовірностей $P(v,h)$ відповідає розподілу Больцмана. Встановивши початкові значення прихованого шару, ймовірність видимого шару P(v|h) може бути визначена за рівняннями

$$P\left(v|h\right)=\prod_i P\left(v_i|h\right),\ P\left(v=1|h\right)=\frac{1}{1+exp\left(-\sum_j w_{ij}h_j-c_i\right)}, \quad (1)$$

де w_i – ваговий коефіцієнт; c_i – зсув прихованого шару, а функція активації – сигма-функція. Процес навчання моделі DBN полягає в постійному оновленні вагових параметрів $\{w_1, w_2, \ldots, c_1, c_2, \ldots\}$ з метою максимізації розподілу ймовірностей P(v,h) вектора видимого шару v і прихованого шару h [4].

Процес виявлення інсайдерської загрози на основі адаптивної оптимізації DBN включає 4 основних етапи: 1) формування журналів поведінки користувачів; 2) попередня обробка записів журналів; 3) глибоке вивчення особливостей поведінки та пошук аномалій; 4) класифікація моделей поведінки та виявлення інсайдера [5].

Використання моделей глибокого переконання дає можливість виявляти приховані зв'язки та відшукувати паралелі у подіях. Навчання DBN на основі алгоритмів адаптивної оптимізації дає змогу досягти ефективності розпізнавання ситуацій на рівні 91 – 92 %. Напрямом подальших досліджень моделей DBN для виявлення інсайдерських загроз може бути розробка алгоритмів навчання моделі в умовах сильної зашумленості початкових даних, наявності у статистиці пропущених даних, застосування методу в умовах умисного спотворення варіантів поведінки користувачів.

Література

1. 2020 Insider Threat Report. Retrieved from: https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf.

2. Мартьянов Е.А. Возможность выявления инсайдера статистическими методами // Системы и средства автоматики. –2017, т. 27, № 2. – С. 41– 47.

3. Hinton G.E. A practical guide to training restricted Boltzmann machines. In: Montavon G, editor. Neural Networks: Tricks of the Trade 2012. 2nd ed. Berlin, Germany: Springer. pp. 599-619.

4. Salakhutdinov R, Hiton G. An efficient learning procedure for deep boltzman machines. Neural Comput 2012; 24: 1967-2006.

5. Савченко В.А. Нейромережева технологія виявлення інсайдерських загроз на основі аналізу журналів активності користувачів. Савченко В.А., Савченко В.В., Довбешко С.В., Мацько О.Й., Зідан А.М. // Сучасний захист інформації №4(36), 2018. – С. 40-49.

УДК 004.056.5

Сапожнік Т.М.
Пахольченко Д.В.
Бакалинський О.О.
кандидат технічних наук,
Адміністрація Державної служби спеціального зв'язку
та захисту інформації України

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ АСУ ТП

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору.

Кіберпростір – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Одним із важливих завдань для держави є забезпечення кіберзахисту об'єктів критичної інфраструктури держави, до яких відносяться підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей [1].

Разом з тим, стале функціонування об'єкта критичної інфраструктури забезпечують об'єкти критичної інформаційної інфраструктури. До таких об'єктів відноситься комунікаційні або технологічні системи об'єктів критичної інфраструктури, кібератака на які безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [1].

Аналіз законодавства України показує, що на сьогодні розроблена низка нормативно-правових актів, які регулюють питання пов'язані із забезпеченням кіберзахисту комунікаційних систем об'єктів критичної інфраструктури.

Велика кількість промислових об'єктів, які потенційно можуть бути ідентифіковані, як об'єкти критичної інфраструктури використовують технологічні системи, що дозволяє підвищити ефективність виробництва, оптимізувати використання ресурсів, зменшити вплив людського фактору на виробництво, якісно виконувати складні завдання, контролювати роботу систем завдяки обробці та архівації даних. Більшої актуальності набирає процес автоматизації та «інтелектуалізації» таких систем. При цьому розробка нормативно-правових актів та стандартів із забезпечення кібербезпеки, їх функціонування, дещо відстає від розвитку та поширення таких систем, а відповідно з цим, затримується розробка суто технічних методів із кіберзахисту та їх практична реалізація, не сформовані підходи до управління ризиками при впровадженні та подальшій експлуатації АСУ ТП.

Необхідно зауважити, що ще в 2018 року Міжнародною електротехнічною комісією (IEC) було розроблено серію стандартів ISA/IEC 624433. Метою розробки цієї серії було впровадження уніфікованого термінологічного апарату, який застосовується при описанні процесів впровадження та

підтримання функціонування систем управління технічним процесом, дотримання правил та вимог забезпечення безпеки, захист від кібератак таких систем.

Серія стандартів ISA/IEC 62443 – це багатогалузева ініціатива, що застосовується до всіх ключових галузей промисловості, критичної інфраструктури, забезпечує гнучку основу для усунення та пом'якшення поточних і майбутніх вразливих місць безпеки в промислових системах автоматизації та управління. Розроблені, на основі знань та досвіду міжнародних експертів з питань кібербезпеки в промисловості, уряду та наукових шкіл, стандарти являють собою комплексний підхід до кібербезпеки [2].

Стандарт розглядає кібербезпеку як постійний процес, а не як мету, яку потрібно досягти, і забезпечує розробку компонентів IACS, які є захищеними від кібератак. Інтеграція цих компонентів у промислове середовище повинна регулюватися глибокою політикою та практичним захистом.

Всі стандарти та технічні звіти ISA-62443 організовані у чотири категорії, що називаються Загальні, Політика та Процедури, Система, Компонент [3].

Основними стандартами серії IEC 62443 є такі [3]:

– IEC 62443-2-4, охоплює політику та практику інтеграції системи;
– IEC 62443-3-3, охоплює вимоги та рівні безпеки;
– IEC 62443-4-1, охоплює вимоги безпечного життєвого циклу розвитку;
– IEC 62443-4-2, охоплює технічні характеристики безпеки компонентів IACS.

В Україні перекладений та прийнятий лише один стандарт із серії ISA/IEC 62443 – ДСТУ EN IEC 62443-4-1:2019 Безпечність систем промислової автоматизації та керування. Частина 4-1. Вимоги до життєвого циклу розроблення безпечної продукції, затверджений наказом ДП «УкрНДНЦ» від 13.08.2019 № 249 «Про прийняття національних стандартів та прийняття поправки до національного стандарту».

Висновки. Важливим кроком для України, який допоміг би не відставати у розвитку від провідних країн та підвищити кіберзахист критичної інфраструктури держави, є розробка та впровадження власних стандартів, нормативно правових документів на основі міжнародних, в тому числі із питань, які стосуються безпеки управління технічних процесом. Для приведення у відповідність термінів необхідно насамперед розглянути та прийняти стандарт ISA-62443-1-1, де описуються основні поняття та моделі, пов'язані з кібербезпекою технічних систем, а також інші три основні стандарти серії IEC 62443-2-4, IEC 62443-3-3, IEC 62443-4-2.

В зв'язку з особливостями функціонування АСУ ТП, їх відмінностями від звичайних ІТС виникає необхідність перегляду підходів для управління ризиками інформаційної/кібербезпеки, їх функціонування.

Актуальним є завдання розробки формальних моделей, які описують безпечне функціонування АСУ ТП, та методів забезпечення їх кібербезпеки.

Література

1. Верховна Рада України. 7 сесія. (2017, жовт. 5). Закон № 2163-VIII, Про основні засади забезпечення кібербезпеки України. [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/laws/show/2163-viii.

2. ISA/IEC 62443 Cybersecurity Certificate Programs [Електронний ресурс] – Режим доступу до ресурсу: https://www.isa.org/training-and-certification/isa-certification/isa99iec-62443/isa99iec-62443-cybersecurity-certificate-programs.

3. DesRuisseaux D. Cybersecurity Assessment – The Most Critical Step to Secure an Industrial Control System [Електронний ресурс] / Daniel DesRuisseaux // Version 1.0. – 7. – Режим доступу до ресурсу: https://www.se.com/us/en/download/document/998-20298472/.

4. Kilian M. IEC62443 in a nutshell [Електронний ресурс] / Marty Kilian. – 2019. – Режим доступу до ресурсу: https://certx.com/wp-content/uploads/2019/03/SCSD19-CertX_IEC62443_in_a_nutshell_published.pdf2.

УДК 1:316.4

Тимошенко Р. Р.
кандидат технічних наук
Загородніх В. В.
Войтех К. Р.
Національний університет оборони України
імені Івана Черняховського

ДЕЯКІ АСПЕКТИ ІЄРАРХІЧНОЇ СИСТЕМИ ПРОТИДІЇ КІБЕРЗАГРОЗАМ У ЗБРОЙНИХ СИЛ УКРАЇНИ

Національна система кібербезпеки є сукупністю 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 [1].

Основними суб’єктами національної системи кібербезпеки є 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. Так відповідно до Конституції і законів України Міністерство оборони України, Генеральний штаб Збройних Сил України

здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони). Здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз. Впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану [2].

Тому на Міністерство оборони України та Генеральний штаб Збройних Сил України покладається завдання щодо забезпечення кібербезпеки у межах своєї компетенції, а саме:

здійснювати заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

здійснювати виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

здійснювати інформаційний обмін щодо реалізованих та потенційних небезпечних кіберзагроз;

розробляти і реалізувати запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

забезпечувати проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

здійснювати інші заходи із забезпечення розвитку та безпеки кіберпростору.

Тому при Генеральному штабі був створений кіберцентр якій відповідає за інформаційну безпеку в ЗС України та на нього покладені завдання щодо забезпечення функціонування та захист від кіберзагроз як інформаційних ресурсів так і серверного та комутаційного обладнання та надання допомоги та контролю щодо забезпечення кібербезпеки інформаційної безпеки віддалених військових частин та навчальних закладів ЗС України.

Обов'язки щодо кібербезпеки відкритих каналів зв'язку у військових частинах та навчальних закладах МОУ покладені на вузли зв'язку які працюють з визначеними керівними документами провайдерами (ISP) які надають доступ до глобальної мережі Інтернет. Цей сегмент є найбільш уразливий для кібератак у зв'язку з тим що відповідальні особи які займаються даним питанням як правило ні є фахівцями у даному питанні та потребують проведення з ними додаткових занять (вивчення налаштування комутаційного обладнання та фаєрволів, ведення статистики мережевого трафіку та вміння реагувати на основні кібератаки) або надання відваленої допомоги кіберцентром під час налаштування комутаційного обладнання, фаєрволів та надалі супроводження інформаційної мережі.

Проблеми захисту інформаційної інформаційних систем які повинні бути розв’язані дозволяють підвищити відмовостійкість та кібербезпеку підрозділів ЗС України:

захист інформаційної інфраструктури;

захист програмного забезпечення;

захист апаратної частини включаючи захист інформації в локальних обчислювальних мережах передачі даних;

управління системою моніторингу та системою запобіганню вторгнення (Intrusion Prevention System, IPS).

Тому при вирішуванні наступних питань інформаційної безпеки повинні виконуватись наступні етапи створення засобів захисту інформації:

визначення апаратно-програмних ресурсів, що підлягають захисту;

оцінювання інформаційних каналів витоку інформації та їх ризиків;

визначення вимог до системи протидії та моніторингу, та контроль її цілісності;

оптимальний вибір засобів передачі та захисту інформації;

Таким чином ієрархічна система протидії кіберзагрозам дозволяє забезпечити оптимальними часові та якісними показниками захисту та відмовостійкості інформаційної мережі ЗС України.

Література

1. Законі України Про основні засади забезпечення кібербезпеки України (Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403) {Зі змінами, внесеними згідно із Законом № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст. 241}.

2. Законі України "Про оборону України" (Відомості Верховної Ради України, 2000 р., № 49, ст. 420; 2011 р., № 4, ст. 27; 2015 р., № 16, ст. 110; 2016 р., № 33, ст. 564).

УДК 621.3

Цмоканич І.В.
Крючкова Л.П.
доктор технічних наук, доцент,
Державний університет телекомунікацій

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИСОКОЧАСТОТНОГО НАВ’ЯЗУВАННЯ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

На сьогоднішній день є актуальною проблема захисту інформації від витоку на об’єктах критичної інфраструктури. Враховуючи тенденції, це питання є особливо важливим в розрізі управління інформаційною безпекою держави. Засоби та заходи для перехоплення інформації, зокрема шля-

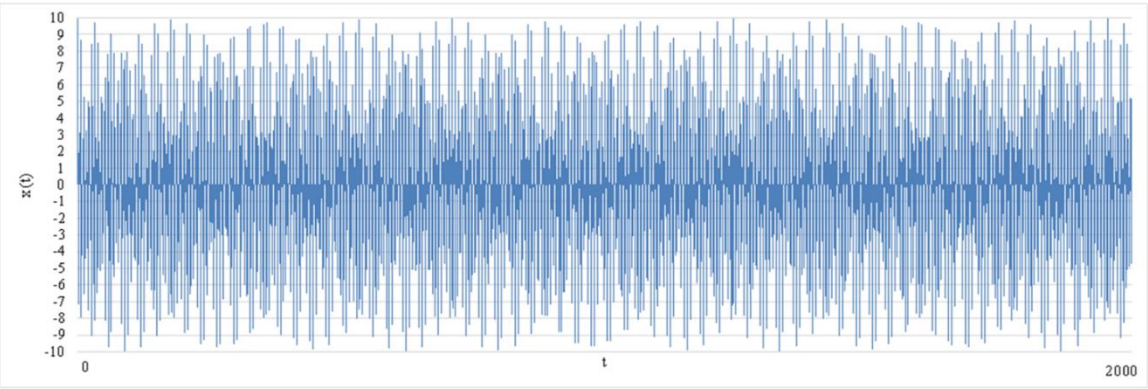
хом високочастотного нав’язування, постійно вдосконалюються, тому потрібно проводити модернізацію заходів щодо забезпечення захисту інформації.

Однією з найбільших загроз для інформації, яка обробляється на об’єктах критичної інфраструктури, є витік інформації технічними каналами (ТКВІ) [1].

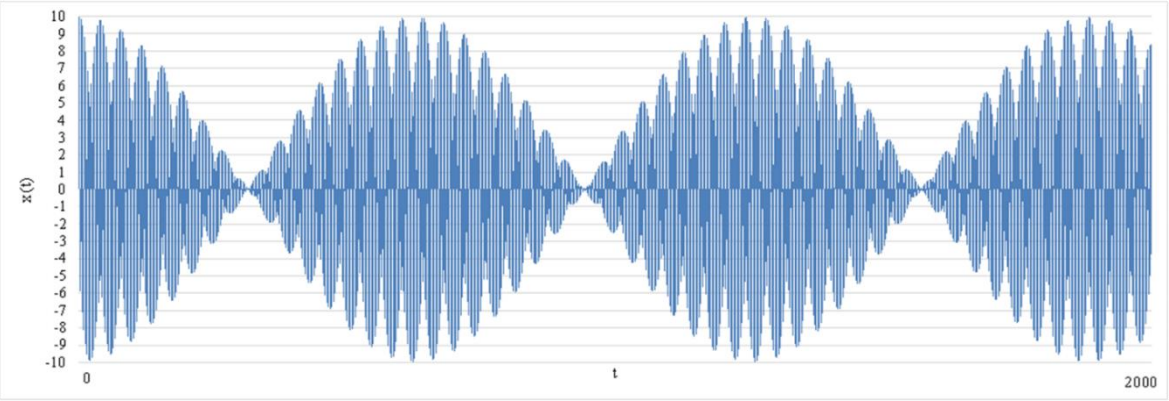
Серед ТКВІ розглянемо канал високочастотного (ВЧ) нав’язування. Канал ВЧ нав’язування утворюється шляхом модуляції сигналів ВЧ генераторів та/або генерації підсилювачів. Канал ВЧ нав’язування утворюється шляхом модуляції небезпечним сигналом високочастотних сигналів ВЧ генераторів ОТЗС, випромінювання модульованих ВЧ коливань у вільний простір та перехоплення таких коливань радіоприймальними пристроями засобів технічної розвідки за межами контрольованої зони (КЗ). Відповідно в другому варіанті канал утворюється шляхом самозбудження підсилювачів низької частоти ОТЗС на гармоніках, кратних небезпечному сигналу, поширення їх у вигляді поля електромагнітного випромінювання за межі КЗ та перехоплення цього поля радіоприймальними пристроями засобів технічної розвідки. Задля забезпечення захисту інформації від витоку використовується ВЧ генератор, метою якого є «накладання» ще однієї частоти, яка спотворює небезпечний сигнал, обумовлений ВЧ нав’язуванням. Цим методом досягається так зване «биття» частот. Проблемою такого генератора є те, що потрібно вести контроль за частотою, яку він генерує, та змінювати її відповідно до того, як змінюється частота сигналу ВЧ нав’язування [2].

Задля вирішення цієї проблеми було проведено дослідження щодо пошуку оптимальних параметрів сигналу ВЧ генератора у відповідності до небезпечного. Для цього було використано середовище для математичних та інженерних обчислень Mathcad 14.

Як видно на рис. 1, при $|\omega1-\omega2|=1$ МГц, де $\omega1$ – частота небезпечного сигналу, а $\omega2$ – частота сигналу, який задається генератором, «биття» частот практично відсутнє та не забезпечує бажаного результату. Слід зазначити, що $\omega1= 800$ МГц в цьому експерименті.



Натомість при |ω1-ω2|=0,01 МГц можна чітко побачити «биття» частот, що в свою чергу свідчить про забезпечення захисту інформації від витоку (рис. 2).



Висновки: задля забезпечення захисту інформації від витоку каналами ВЧ нав'язування можна використовувати генератор, який буде забезпечувати «биття» частот, тим самим унеможливлюючи перехоплення інформації. Як показало дослідження, найбільш ефективне використання генератора спостерігається при 0,1≤|ω1-ω2|≤0,15 МГц. Дане правило спостерігається і при інших частотах небезпечного сигналу, що дає можливість стверджувати, що такий спосіб використання генератора є дієвим для забезпечення захисту інформації від витоку на об'єктах критичної інфраструктури.

Література

1. Про критичну інфраструктуру та її захист. Проект закону України від 27.05.2019 №10328. [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/JH7YW00A.html (дата звернення: 4.03.2021).

2. Патент 95365 Україна, МПК (2011.01) H04K 3/00. Спосіб захисту інформації / Рибальський О.В., Хорошко В.О., Крючкова Л.П., Джужа О.М., Орлов Ю.Ю.; заявник і патентовласник Національна академія внутрішніх справ. - № a200913327; заявл. 22.12.2009; 55 опубл. 25.07.2011, Бюл. № 14.

УДК 355.40:041

Цурко Ю.В.
Національний університет оборони України
імені Івана Черняховського

ФАКТОРИ, ЯКІ ВПЛИВАЮТЬ НА СТАН КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У сучасному суспільстві кібератаки стають частішими та мають тенденцію чинити все значніший і триваліший вплив на економіку країни, незаперечним є той факт, що надійний захист від кібератак активно впливає на

стан економічної, політичної, соціальної, оборонної та інших складових національної безпеки держави [1].

Очевидним є той факт, що порушення функціонування об'єктів критичної інфраструктури держави може призвести до розвитку надзвичайних ситуацій, пов'язаних із загибеллю людей, екологічними катастрофами, заподіянням великого матеріального, фінансового, економічного збитку або великомасштабними порушеннями життєдіяльності міст та населених пунктів. У цих умовах надзвичайно важливу роль відіграє забезпечення безпеки, у тому числі і кібербезпеки об'єктів критичної інфраструктури держави.

Враховуючи зазначене вище, метою тез є визначення основних факторів, що впливають на стан кібербезпеки об'єктів критичної інфраструктури.

Проведений аналіз існуючих систем захисту інформації, дає змогу визначити основні складові частини системи кіберзахисту інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури [2]:

нормативно-правова;

організаційна;

технічна;

підготовка, перепідготовка та підвищення кваліфікації відповідних фахівців.

Кожна із приведених вище складових частин, так чи інакше, впливає на стан кібербезпеки ІТС ОКІ.

ІТС зазвичай являються об'єктом захисту, як цілісні утворення. В той же час, їх складові елементи: обслуговуючий персонал, математичне, програмне, технічне, інформаційне забезпечення тощо можливо розглядати, як окремі об'єкти захисту від кіберзагроз.

Кіберзагрози для ІТС можуть виходити з різних джерел: навмисних, ненавмисних, природних [3].

Джерела кібератак для інформаційних систем об'єктів критичної інфраструктури можуть знаходитись як ззовні (зовнішній порушник) так і зсередини.

Відповідно проведеного аналізу, на стан забезпечення кібербезпеки ІТС об'єкта критичної інфраструктури можуть впливають такі фактори:

наявність необхідної та достатньої нормативно-правової бази з питань забезпечення кібербезпеки ІТС об'єктів критичної інфраструктури;

наявність джерел кіберзагроз, їх можливості, тип, вид, мета, мотиви, зацікавленість у здійсненні кібератак;

наявність вразливостей у системах кіберзахисту, які можуть використовуватися при здійсненні кібератак;

наявність чи відсутність сприятливих умов для реалізації кіберзагроз;

привабливість активів, на які власне і спрямовуються кібератаки;

наслідки від можливої реалізації кіберзагроз;

рівень фахової підготовки співробітників, відповідальних за кібербезпеку на всіх рівнях: організація, підприємство, галузь, відомство тощо.

Також, одним із таких показників може бути кількість кібератак за певний інтервал часу – рік, півріччя, квартал, місяць.

Крім того, одним із суттєвих показників може бути спрямованість кібератак – органи державної влади, енергетика, банківська сфера, об'єкти сектору безпеки і оборони, відомства, дипломатичні установи тощо.

Таким чином, кібербезпека є невід'ємною складовою інформаційної 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 та інформаційно-технологічної безпеки держави.

Література

1. А.Крутских, А.Федоров "Про міжнародну інформаційну безпеку, Міжнародне Життя", № 2, 2010.

2. В.В. Домарев "Безопасность информационных технологий. Методология создания систем защиты." Киев, Украина: ООО "ТИД "ДС", 2002.

3. С.Гончар, Г.Леоненко "Аналіз факторів впливу на стан кібербезпеки інформаційної системи об'єкту критичної інфраструктури". Information Technology and Security. July-December 2016. Vol. 4. Iss. 2 (7).

УДК 004.056

Штонда Р.М.
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут

АЛГОРИТМ ДІЇ АДМІНІСТРАТОРА БЕЗПЕКИ У РАЗІ ВИЯВЛЕННЯ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ВІРУСУ ШИФРУВАЛЬНИКА

У 2013-2017 роках кібератаки проти України здійснювалися з використанням APT-атак. Перші системні атаки були зафіксовані у травні 2014 року на об'єкти критичної інфраструктури України. Також відбулися кібератаки на енергетичний сектор: у грудні 2015 року – на ПрАТ "Прикарпаттяобленерго" і ПрАТ "Київобленерго"; у грудні 2016 року – на компанію "Укренерго". У червні 2017 року деякі об'єкти критичної інфраструктури України зазнали атаки комп'ютерного вірусу Petya.

Тому існує необхідність створення алгоритму для протидії вірусу шифрувальнику (далі – ВШ). Важливість створення даного алгоритму полягає в тому, що спостерігається постійне просування нових зразків ВШ типу

Petya по всьому світу та нажаль до низки об'єктів критичної інформаційної інфраструктури України.

Алгоритм дій адміністратора безпеки щодо протидії ВШ [1]:

заздалегідь завантажити в інформаційно-телекомунікаційну систему (далі – ІТС) актуальні зразки спеціального програмного забезпечення (далі – СПЗ) з функціями антивірусного захисту;

завантажити в ІТС СПЗ яке здатне виявляти ознаки несанкціонованого шифрування, призупинення процесів та CPU, копіювання інформації з ОЗУ та HDD, пошуку ключів, відновлення і розшифрування інформації та відновлення ІТС;

забезпечити роботу ІТС згідно її функціоналу;

налаштувати роботу СПЗ необхідного для виявлення ознак дії ВШ в ІТС;

забезпечити постійне "чергування" вищевказаного СПЗ в системі;

у випадку своєчасного виявлення ознак ВШ здійснити блокування ВШ;

відновити працездатність ІТС згідно її функціоналу.

при необхідності здійснити пошук ключів для розшифрування інформації.

У випадку коли ознаки шифрування виявлені, адміністратор безпеки здійснює наступні дії:

знищує шкідливі процеси в ІТС;

здійснює копіювання образу інформації ІТС;

завантажує образи ІТС на станцію кіберекспертизи типу Ntb HP "G7/8";

здійснює спробу крипто аналізу алгоритму шифрування;

здійснює пошук сигнатур ВШ;

здійснює пошук ключів шифрування в образах інформації;

здійснює розшифрування та відновлення файлів;

здійснює відновлення операційної системи, додатків та даних ІТС;

розробляє звіт про інцидент в ІТС;

приймає участь в аналізі шляхів зараження ІТС.

Для унеможливлення роботи ВШ в ІТС доцільно заздалегідь підготувати СПЗ та забезпечити повну обізнаність адміністраторів безпеки, а саме: досягати повної обізнаності адміністраторів та користувачів ІТС щодо загрози від ВШ та постійно відпрацьовувати їх практичні навички із протидії загрозам дій ВШ; постійно оновляти актуальне СПЗ для можливості ефективного блокування початку роботи ВШ; постійно резервувати інформацію системи, щоб у вас було декілька бекапів: один у хмарі, наприклад Dropbox, Google Drive та інших спеціалізованих сервісах, а також на змінному носії; проводити навчання для підвищення навичок адміністраторів безпеки щодо практичної нейтралізації дії ВШ.

Література

1. Куцаєв В.В., Штонда Р.М., Терещенко Т.П., Артемчук М.В., Нещерет І.Г. Алгоритм блокування вірусу шифрувальника в інформаційно-телекомунікаційних системах. Збірник наукових праць ВІТІ. Київ, 2020. Вип. №3, с. 43-55.

УДК 004.056.5
Ящук В.І.
кандидат економічних наук, доцент,
Львівський державний університет безпеки життєдіяльності

ПРОЕКТУВАННЯ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

В останні роки в Україні активно обговорюється створення державної системи захисту критичної інфраструктури. З 2016-го спостерігається збільшення випадків диверсії та терористичних загроз спрямованих на об'єкти критичної інфраструктури України. Попри це, в країні досі немає ні законодавчого визначення критичної інфраструктури, ні офіційного переліку таких об'єктів. Відтак, набув чинності Порядок формування переліку об'єктів критичної інформаційної інфраструктури [1].

Сьогодні об'єктами критичної інфраструктури вважаються підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв [1].

Об'єкти критичної інформаційної інфраструктури - це власність суб'єктів критичної інформаційної інфраструктури (підприємства - власники таких об'єктів): інформаційні системи (ІС); інформаційно-телекомунікаційні мережі (ІТКМ); автоматизовані системи управління (АСУ).

Таким чином, передбачено два види суб'єктів критичної інформаційної інфраструктури - власників об'єктів критичної інформаційної інфраструктури та координаторів взаємодії цих об'єктів.

Захисту об'єктів критичної інформаційної інфраструктури вимагає застосування системного підходу. Комплекс робіт із захисту об'єктів критичної інформаційної інфраструктури містись:

– проведення процедур класифікації об'єктів критичної інформаційної інфраструктури;

– аналіз інформації щодо безпеки та розроблення моделей інформації про безпеку;

– проектування та впровадження системи захисту об'єктів критичної інформаційної інфраструктури;

– розробка робочих (експлуатаційних) документацій на об’єкті (у частині забезпечення його безпеки);

– розробка організаційно-розпорядчих документів, регламентуючих правил та процедур забезпечення безпеки об’єкта;

– впровадження організаційних заходів із забезпечення безпеки об’єкта;

– навчання співробітників, що відповідають за безпеку об’єктів критичної інформаційної інфраструктури.

Автоматизована інформаційна система управління кібернетичною безпекою, як правило, створюється не для певного підприємства і потребує певної адаптації під потреби та вимоги конкретного об’єкту критичної інфраструктури. Проте, є багато спільних рис в структурі об’єкту критичної інфраструктури, а також в типах зв’язків (функціональних, інформаційних, зовнішніх) між елементами цієї структури. Це дозволяє сформулювати єдині принципи і шляхи побудови автоматизованих інформаційних систем управління кібернетичною безпекою об’єктів критичної інфраструктури.

Виділимо етапи створення і функціонування (життєвого циклу) автоматизованих інформаційних систем управління кібернетичною безпекою об’єктів критичної інфраструктури України: 1) розроблення концепції автоматизованої інформаційної системи управління об’єктами критичної інфраструктури, 2) розроблення технічного завдання, 3) проектування, 4) реалізація, 5) впровадження в експлуатацію (тестування і налагодження), 6) супровід.

На першому етапі проводиться обстеження об’єкта, вивчаються форми вхідних та вихідних документів, методики розрахунків необхідних показників. Проводяться також науково-дослідні роботи щодо оцінювання реалізації вимог замовника: здійснюється підбір необхідних засобів моделювання процесів, які комп’ютеризуються, пошук відповідних програмних засобів, оцінка альтернативних проектів.

На цьому ж етапі розробник погоджує із замовником вимоги до ІС, її функції, необхідні витрати на розробку, терміни виконання. Завершується перший етап складанням звіту про проведені роботи, на основі якого в подальшому буде розроблено технічний проект.

На другому етапі формується технічне завдання, яке є підставою для розробки інформаційної системи і приймання її в експлуатацію. Воно визначає основні вимоги до самої системи та процесу її розробки і розробляється для системи в цілому. Додатково можуть розроблятись технічні завдання на окремі частини автоматизованої інформаційної системи управління готелями.

На третьому етапі розробляється концепція інформаційної бази, створюється інфологічна і даталогічна моделі, формуються вимоги до струк-

тури інформаційних масивів, технічних засобів. Вказуються характеристики програмного забезпечення, систем класифікації та кодування. Результатом даного етапу є комплект проектної документації (технічний проект). В ньому вказується постановка задачі, алгоритм її розв'язання, описується інформаційне, організаційне, технічне та програмне забезпечення, тощо. Після затвердження технічного проекту розробляється робочий проект (внутрішній). Одночасно з розробкою проекту створюються класифікатори техніко-економічної інформації на основі погодженої системи класифікації і кодування техніко-економічної інформації.

На четвертому етапі здійснюється розробка програмного забезпечення у відповідності з проектною документацією. Результатом цього етапу є готовий програмний продукт.

На п'ятому етапі проводиться перевірка програмного забезпечення на предмет відповідності вимогам, вказаним в технічному завданні. Дослідна експлуатація (тестування) дозволяє виявити недоліки, які можуть появитись при експлуатації системи. На цьому ж етапі проводиться підготовка персоналу до роботи в інформаційній системі. Навчання персоналу здійснюється або силами розробника, або за допомогою спеціальних курсів. Підготовлюється робоча документація, проходять приймальні випробування, і система здається в експлуатацію замовнику.

Шостий етап організовується на підставі гарантійних зобов'язань розробника. У цей період здійснюється сервісне обслуговування системи, усуваються недоліки, які можуть бути виявлені при експлуатації, і завершуються роботи по даному проекту. Всі етапи розробки і впровадження ІС повинні бути обумовлені у відповідних угодах між замовником і розробником, а також у технічному завданні.

Література

1. Порядок формування переліку об'єктів критичної інформаційної інфраструктури затверджений Постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text (дата звернення: 10.03.2021).

2. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури затверджені Постановою Кабінету Міністрів України від 19 червня 2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8 (дата звернення: 10.03.2021).

НАУКОВЕ МАЙБУТТЯ
УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ ОЧИМА МОЛОДИХ ВЧЕНИХ, СТУДЕНТІВ, КУРСАНТІВ

УДК 351.86
Березньова А.О.
Національна академія Служби безпеки України

КОРУПЦІЯ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Корупція – це злочин проти держави та громадянина, вона загрожує сприйняттю законних дій державних органів та безпеці громадян, негативно впливає на репутацію органів державної влади, перешкоджає реформуванню державного управління. Тому питання запобігання та боротьби з корупцією є важливим, його потрібно вирішувати в рамках реформи держави та соціально-політичних процесів. Фахівці з політології, соціології, юриспруденції, державного управління активно розглядають та обговорюють проблеми запобігання та протидії корупції, формують базу даних осіб, які вчинили корупційні дії або пов'язані з корупційними правопорушення, встановлюючи пріоритети для розвитку антикорупційної політики. Рівень корупції в Україні впливає не тільки на соціально-економічний розвиток, добробут населення, довіру громадян до органів державної влади, а й загрожує національній безпеці держави. Крім того, корупція уповільнює сучасні процеси реформ у системі управління, які мають на меті покращити життєздатність суспільства, забезпечити економічний розвиток, сформувати позитивний імідж держави на міжнародній арені.

За останній рік показники України в Індексі сприйняття корупції (Corruption Perceptions Index – CPI) виросли на 3 бали. Із 33 балами зі 100 можливих ми отримали 117 місце зі 180 країн у списку CPI. Поруч із нами у рейтингу Єгипет, африканська Есватіні (Свазіленд), Непал, Сьєрра-Леоне та Замбія – всі ці країни так само у CPI-2020 набрали по 33 бали [1].

Можна виділити такі типи стратегій політики державної безпеки: 1) орієнтовані на усунення існуючих або запобігання виникненню можливих загроз; 2) спрямовані на запобігання впливу існуючих або потенційних загроз безпеці; 3) спрямовані на відновлення (відшкодування) збитків. Таким чином, ефективні стратегії спрямовані на запобігання виникненню можливих загроз, що передбачає розробку спеціальних методів прогнозування для виявлення потенційних загроз безпеці держави. Перші два типи стратегій передбачають безпекову діяльність, яка не становить загрози або створює бар'єр для її впливу. У третьому випадку шкода допускається, але вона відшкодовується діями, передбаченими стратегією. Зрозуміло, що

стратегії третього типу можуть розроблятися і реалізовуватися в ситуаціях, коли збитки можуть бути компенсовані, або коли неможливо реалізувати стратегію першого або другого типу [2].

До основних проблем політики безпеки в контексті запобігання та протидії корупції належать: політичні (несприятливі характеристики політичної еліти, політична нестабільність, недосконаліть механізмів відносин між органами державної влади та політичними партіями, відсутність стабільних традицій демократії, недоліки, надмірна політична децентралізація); економічні (надмірне втручання держави в економіку, недоліки системи оплати праці державних службовців, неадекватна податкова політика, низький рівень економічного розвитку, висока доступність природних ресурсів тощо); соціальні (низька освіченість суспільства, слабкість громадянського суспільства тощо); правові (недорозвинене антикорупційне законодавство, прогалини в правовому регулюванні суспільних відносин, невідповідність між положеннями різних нормативних актів, незрозумілі мовні формулювання правових норм, винятки із загальних прав та процедур, плутанина та розпорошеність правового регулювання тощо.); управлінські (слабка ефективність державного контролю, структурні та функціональні недоліки системи державних органів, непрозорість їх діяльності, безладна загальна адміністративна процедура, нерозвиненість адміністративного судочинства, відсутність належного організаційного забезпечення антикорупційної діяльності, недоліки в наданні адміністративних послуг); психологічні (поява корупційних стереотипів через засоби масової інформації, гіперболізація в суспільній свідомості тотальної корупції державного апарату, поширення ідеї марності корупції особистості тощо); культурно-етичні (відсутність надлишкових цінностей, ідеалів та моральних заборон, відмінності між суспільним сприйняттям корупції та її юридичним визначенням, існування подвійних моральних стандартів корупції, нерозуміння тяжкості корупції в суспільстві) [3].

До основних елементів системи політики безпеки України в контексті запобігання та протидії корупції слід віднести: об’єкти та суб’єкти державної безпеки; методи забезпечення державної безпеки; механізми забезпечення державної безпеки, а також зовнішні та внутрішні загрози.

Таким чином, корупція - це протиправна дія чи бездіяльність посадової особи (або особи, наділеної певними адміністративними повноваженнями та функціями), яка спрямована на отримання власних інтересів (як матеріальних, так і нематеріальних, включаючи певні послуги, привілеї, пільги тощо) шляхом здійснення їх функціональних обов’язків та негативно впливає на державу, суспільство та органи державної влади. Корупція не тільки має негативні наслідки для суспільства, але і впливає на репутаційний капітал органів державної влади та шкодить національній безпеці держави.

Література

1. Україна в Індексі сприйняття корупції-2020 URL: http://cpi.ti-ukraine.org/

2. Пархоменко-Куцевіл О. Формування політики державної безпеки України в контексті запобігання та протидії корупції. Державне управління та місцеве самоврядування, 2019, вип. 1(40). С. 90-95

3. Антикорупційна політика та запобігання корупції в публічному управлінні : навч. посіб. / І. С. Бондар, В. Г. Горник, С. О. Кравченко, В. В. Кравченко. Київ : Ліра-К, 2016. С. 78 – 94.

УДК 004.056

Бржевська З.М.
Державний університет телекомунікацій

УЗАГАЛЬНЕННЯ МОДЕЛІ ОЦІНКИ РИЗИКІВ ПОРУШЕННЯ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ

Порушення достовірності інформації несе в собі ризики для держави. Оцінювання таких ризиків являє собою достатньо складне завдання. Розглянемо підхід щодо оцінювання та нейтралізації ризику, пов'язаного з впливом ФІП.

Нехай існує скінчена множина ФІП, які характеризуються відносними частотами виникнення $p_l^{\text{ФІП}}$ і збитком, що наноситься підприємству u_l, де $l = \overline{1,n}$. СЗДІ виконує функцію протидії порушення достовірності ІР. Основною характеристикою засобу забезпечення достовірності є можливість збереження достовірності ІР кожного *i*-го ІР при впливі на нього *l*-го ФІП p_{il}^c.

Збиток ІП при відсутності СЗДІ може бути представлений як сумарний по кожному ФІП [2, 5-7]

$$U=\sum_{l=1}^{n} U_l \tag{1.1}$$

Ризик для ІП при відсутності СЗДІ являє собою функцію відносних частот виникнення ФІП і збитку в разі порушення достовірності

$$R^{\text{НЗ}} = f(p_l^{\text{ФІП}}, u_i)=\sum_{l=1}^{n} p_l^{\text{ФІП}} * u_i \,, \tag{1.2}$$

З огляду на імовірнісний характер ФІП, можна замінити відвернений збиток $\Delta W=U-W$ на усунутий ризик $\Delta R=R^{\text{НЗ}} - R^{\text{ЗАХ}}$ [2]. Тоді економічна ефективність функціонування СЗДІ може бути визначена як

$$\text{Ef}=\frac{R^{\text{НЗ}}-R^{\text{ЗАХ}}}{S_{\text{СЗД}}} = \frac{\sum_{l=1}^{n} p_l^{\text{ФІП}} * u_l * \sum_{l=1}^{n} p_l^{\text{ФІП}} * u_l * \left(1-p_l^{C}\right).}{S_{\text{СЗД}}} \tag{1.3}$$

Для розрахунку економічної ефективності необхідно визначити перелік ІР і їх вартість, а також провести експертизу таких параметрів ІП, як значущості та доступності СУ і ступінь впливу кожного ФІП на все ІР ІП. Достовірна експертиза параметрів ІП можлива тільки на основі визначення повного списку актуальних ФІП та СУ, за умови адекватної оцінки ступеня виконання кількісних і якісних вимог до СЗДІ.

Найбільш складним питанням є оцінка вартості ІР. Нехай вони представлені у вигляді скінченної множини елементів і необхідно оцінити сумарну їх вартість в грошових одиницях.

Запропоновано наступний алгоритм оцінки вартості ІР.

- ресурси, цінність яких є концептуальною, що не приносять безпосередньої прибутку, але втрата або псування яких завдасть підприємству збиток.

1) Оцінка вартості ресурсів починаємо з визначення цінності ІР і 1-й і 2-ї категорії на основі рангової шкали (по табл. 1.1).

Таблиця 1.1

Цінність ІР (по рангової шкалою)

Лінгвістична оцінка цінності ІР на основі розрахунку витрат на відновлення	Значення
Даний ІР є найважливішим для держави. Його втрата завдасть непоправні наслідки для держави.	9
Витрати на ліквідацію наслідків через втрату ресурсу можна порівняти з річними економічними показниками	8
Витрати на відновлення через втрату ресурсу істотні для організації	6
Витрати на відновлення несуттєві, але потрібний додатковий час	2
Відновлення через втрату ресурсу буде проведено в штатному режимі	1

2) групуємо оцінки ресурсів 1-ї категорії так, щоб в кожній з максимум 9 груп (9 градацій в таблиці 3.6) були ресурси з однаковим значенням рангу.

Отриману величину можна вважати вартістю ресурсу, має ранг R. Ряд отриманих величин повинен бути впорядкований по зростанню, і повинна бути виконана умова суттєвої різниці оцінок при істотній відмінності рангів (відповідно до лінгвістичними описами табл. 1.1):

$$\begin{cases} E_R < E_{R+1,} \ (\forall \mathrm{R} = \overline{1{,}8} \\ E_{R_1} << E_{R_2}, (R_2 \geq R_1 + 2)^{\cdot} \end{cases} \quad (1.4)$$

3) Якщо умова (1.4) не виконано, то експерт повинен скорегувати результати.

4) Далі всім IP з 2-ї категорії, які мають ранг R, присвоюємо значення вартості рівне E_R.

$$E_R \xrightarrow[C_i^{\varepsilon}=R]{} S_{\text{ИР.i}}^{\text{2кат}}, (\forall \text{i} = \overline{1, \text{z}_{\text{2кат}}}). \quad (1.5)$$

5) Загальна вартість IP за оцінками ε-го експерта визначаємо підсумовуванням:

$$S_{\text{IP}}^{\varepsilon} = \sum_{\text{i}=1}^{z_{\text{I}}} S_{\text{IP.i}}^{\varepsilon} \quad (1.6)$$

Отже, порушення достовірності інформації несе в собі ризики для підприємств, організацій, чи, у випадку державних інформаційних ресурсів, для держави. Ризик для інформаційних ресурсів при відсутності систем забезпечення достовірності інформації являє собою функцію відносних частот виникнення факторів інформаційного протиборства та завданого збитку в разі порушення достовірності. Ступінь ризику залежить від вартості інформаційних ресурсів, що використовуються у процесах інформаційної взаємодії. Поділ інформаційних ресурсів на дві категорії вартості дає змогу, на основі експертного оцінювання, визначати найбільш доцільні заходи щодо забезпечення достовірності інформації, яка надається такими ресурсами кінцевим споживачам.

Література

1. Виноградов И.М. Основы теории чисел. М.: Наука, 1981. 176 с.
2. ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT, 2013.
3. Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology : NIST 800-30. – Введ. 06.01.2002. – США. – 2002. – 56 с
4. Система управления информационной инфраструктурой: Электронный ресурс.: http://www.incom.ua/products/Softwareintegration/Standartsoftware solutions /sysmanage/index.shtml
5. Common Criteria for Information Technology Security Evaluation. Version 1.0, 96.01.31
6. Federal Criteria for Information Technology Security (FC), Draft Version 1.0, (Volumes I and II), jointly published by National Institute of Standards and Technology and the National Security Agency, US Government, 1993.
7. ISO/IEC 15408-3. Information technology - Security techniques - Evaluation Criteria for IT security - Part 3: Security assurance requirements, 1999.
8. Standards for Information Control Professionals. -ISACA Standards, 2000.
9. An Introduction to Computer Security: The NIST Handbook. Draft ~ National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1994.
10. B. Schneier. Applied Cryptography: Protocols, Algorithms, and Sourse Code in C: Second Edition. John Wiley&Sons, New York, 1996.
11. B. Schneier. Secrets and Lies: Digital Security in a Networked World. John Wiley&Sons, New York, 2000.

УДК 321.011
Вансович Д.В
Фурсенко Д.Г.
Національна академія Служби безпеки України

СУЧАСНІ ВИКЛИКИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

У сучасному світі швидкої цифрової трансформації інформаційні війни, пропаганда продукують недовіру до будь-якої інформації. Отже, Україна повинна бути готова до сучасних викликів і зміна у сфері інформаційної безпеки.

Як зазначають дослідники, традиційне поняття «війна» стає не лише військовим явищем, а й комунікативним. І у сучасному світі все частіше воюють не за територію, а за людську свідомість. «Війна забирає не тільки ресурси, а й інтелект. Всі нові методи та інструментарій, який можна використовувати для бойових дій, відразу ж потрапляють в руки військових зі сфери бізнесу, політики або медіа. А тому Мюнхенська конференція з безпеки 2017 року заговорила про «феномен постправди». Безперечно, постправда вже стала сьогодні інструментарієм війни. Нова парадигма четвертого покоління війни активно на неї спирається», - вважає професор Георгій Почепцов [1].

Відповідно до періодизації поколінь війни Уільяма Лінда, зараз актуальне четверте покоління війни. Російсько-українську війну можна охарактеризувати, як нове покоління війни.

Покоління війни відображають той новий інструментарій, який з'являється на даний час. Третє покоління - це був німецький бліцкриг, що базувався на маневрі, але для цього потрібен був радіозв'язок.

Про четверте покоління війни Лінд говорить, що її характеризує децентралізація і зникнення державної монополії на війну. Саме це дозволяє повернутися до війни культур, а імміграція та мультикультуралізм створюють передумови для війни ідентичностей.

У наш час виникло поняття «постправди», коли завдяки інтернету в нашу голову потрапляє безліч того, що раніше не можна було б собі уявити. Працюють тисячі джерел, відсутня цензура, - все це робить інформаційний потік набагато сильнішим, ніж раніше. Конкретна людина не може його опанувати, бо в ньому весь час виникають «несподіванки».

Тому виникає таке поняття, як фейк, що є спотворенням правди. Він відрізняється від піару чи пропаганди, які все ж зобов'язані базуватися на правді, можливо, її гіперболізуючи.

Фейк не хоче бути правдою, для нього важливіше досягнення власних цілей, а не інформування людини. Разом з тим, зараз у соціальних мережах,

інформаційних виданнях все частіше активізовуються так звані «тролі», які за певну плату виконують те чи інше завдання.

Тролі виконують багато функцій. Одна з них - це створення уявлення, що потрібні меседжі підтримує велика кількість людей. Ще тролі своїми коментами можуть виводити з себе тих, кого їм задають як супротивника. Реально тролі – це намагання держав повернути собі контроль за соціальними медіа.

Наприклад, Фейсбук, що за визначенням є інструментом з індивідуального породження інформації, завдяки тролям отримує «індустріальний» потік інформації, який завжди буде набагато сильнішим, оскільки він несе єдиний меседж.

До речі, сьогодні країни, зокрема такі як Китай, Ізраїль, Росія, мають свої команди тролів, які повинні допомогти їм опанувати вільний чи квазівільний Інтернет.

Як Україні убезпечити свій інформаційний простір від посягань інших держав? Це проблема для будь-якої країни, бо інформаційний простір, на відміну від фізичного, багато в чому спільний, тут важко віднайти кордони. Але є велика асиметрія: ми дивимося американські серіали чи читаємо американські книжки, а вони не дивляться наші фільми і не читають наших книжок.

Свій власний продукт повинен стати найціннішим і найцікавішим для аудиторії. І це зрозуміло - він відображає власну картину світу. Тому державі треба вкладати кошти у створення власних бестселерів і блокбастерів, бо зараз ми практично живемо чужим. Ми дивимося чужі серіали, наші діти читають перекладні книжки, бо не створюємо власного якісного продукту.

Як розвиватимуться інформаційні війни у світі в подальшому? Основне - це довіра до інформації. Тому всі нові методи йдуть у пошуку того, яким чином викликати довіру до власного повідомлення. І сьогодні для цього виникла допомога військовим з боку нейропсихології. Майбутня пропаганда буде набагато ефективнішою, бо вона буде базуватися на об'єктивному типі інструментарію. Тобто пропаганда ускладниться у своїй підготовці, а людина залишиться тою самою (фізіологічно, психологічно), якою була дві тисячі і більше років тому. Модерний інструментарій буде працювати проти незмінного мозку.

У випадку з Росією – це агресивний конфлікт, тому тут є специфічні завдання, а так просувати країну, її власну позицію треба в усьому світі. Одні завдання маємо в Європі, інші - в США. Та і в Європі розмова з країнами Балтії і Польщею буде різною. Це все принципово різні аудиторії. А ще в кожній країні є експертна спільнота, яка впливає на владу, та журналістська спільнота, що впливає на населення. І вони теж повинні отримувати налаштовані саме на них повідомлення [1].

Отже, виходячи з усього вищенаведеного, робимо висновок, що треба нарощувати український контент, як у соціальних мережах, так і на каналах телебачення та радіомовлення. Вкладати кошти у кіноіндустрію, яка б висвітлювала славне українське минуле та формувала єдину думку, як на сході, так на заході країни. Створити міжнародні українські міжнародні канали телебачення, які б могли створювати контент для українців закордоном, а їх різними підрахунками близько двохсот мільйонів, а це в шість разів більше ніж зараз проживає в Україні. Таким чином наші співвітчизники зможуть впливати на інформаційне середовище за межами України, а отже і формувати правильну інформаційну реальність, яка б могла слугувати головним інструментарієм в інформаційній безпеці країни.

Література

1.https://detector.media/withoutsection/article/123918/2017-03-09-georgiy-pocheptsov-viyna-chetvertogo-pokolinnya-tse-viyna-kultur/.

УДК 351

Відьменко Т.Є.
Поліщук Д.В.
Національна академія Служби безпеки України

ФОРМУВАННЯ ПОЗИТИВНОГО ІМІДЖУ УКРАЇНИ В УМОВАХ ВЕДЕННЯ ГІБРИДНОЇ ВІЙНИ

Іміджева складова гібридної війни стала новим викликом для української держави, адже виснажлива інформаційна пропаганда з боку Російської Федерації, а також ризик втрати прихильності на міжнародній арені спонукали представництво країни до зміни геополітичного курсу. Створення системи проактивної державної інформаційної політики, залучення інвестицій, покращення туристичного потенціалу, а також просування національних інтересів стали основоположними принципами організації державної стратегії [2].

Метою цієї публікації є виокремлення та аналіз ключових кроків держави у процесі формування позитивного іміджу України в умовах ведення гібридної війни та інформаційної пропаганди з боку Російської Федерації.

Перш за все, варто відзначити, що формування позитивного іміджу України у світі, донесення оперативної, достовірної і об’єктивної інформації про події в Україні до міжнародної спільноти входять до життєво важливих інтересів суспільства і держави, які закріплені у Доктрині інформаційної безпеки України [3]. Таким чином усі дії, спрямовані на забезпечення ви-

знання України на міжнародній арені, в свою чергу сприяють протидії інформаційно-психологічному впливу Росії на позитивний образ держави. Наразі ми можемо спостерігати активну фазу впровадження технології іміджмейкінгу в усі сфери державної політики. Окрім цього, методи просування позитивного образу держави працюють не лише на зовнішній арені, а й мають внутрішнє спрямування. Наприклад, об'єктивне висвітлення внутрішньодержавних процесів та залучення міжнародної громадськості до участі у різноманітних заходах задля обміну досвідом сприяють зміцненню довіри суспільства та утворенню громадської свідомості.

Протягом останніх шести років значних обертів набирає тенденція до популяризації України у світі. Поштовхом до цієї ініціативи стало дослідження, проведене британським урядом щодо основних реалій, з якими іноземці асоціюють Україну і саме тоді як ніколи гостро постало питання репутації нашої держави та її громадян. ПроєктUkraineNOWстав не лише брендом країни, а й продемонстрував усьому світу відкритість та готовність до змін, продиктованих часом. Наразі під егідою цієї бренд-назви відбувається безліч заходів, проєктів та виставок, які сприяють глобальній зміні уявлень про українське суспільство [4].

У боротьбі на інформаційному майданчику неможливо обійтися без сучасних засобів, а саме соціальних мереж, які є першочерговим важелем впливу насуспільну думку та процеси, які відбуваються всередині країни. Саме тому висвітлення діяльності урядових структур на таких комунікаційних платформах як Facebook, Instagram, Telegramта Twitter є дуже перспективним методом боротьби з фейковими новинами, які стосуються внутрішньополітичних процесів. Більше того, наразі керівництво нашої держави практикує проведення соціологічних досліджень та використання їхніх результатів у процесі державного управління. Такі дії уряду дають змогу об'єктивно оцінювати ситуацію в державі, а також приймати обґрунтовані рішення з урахуванням очікувань громадянського суспільства України.

Сприятливою практикою у процесі формування іміджу України також можна вважати проведення різноманітних форумів, які пропагують методику «відкритого діалогу». Одним з таких заходів є Всеукраїнський форум «Україна 30», створений задля актуалізації критично важливих для українського суспільства питань. Він є дискусійним майданчиком, на якому представники влади всіх рівнів, експертного середовища, громадянського суспільства та міжнародної спільноти піднімають низку проблем, які потребують виважених рішень [1].

Окрім формування образу відкритої держави, Україна також потребує конструктивних змін зсередини. Цьому значною мірою сприяють законодавчі ініціативи, що стосуються популяризації української мови, а саме реформування інститутів ЗМІ, освіти, сфери обслуговування, а також органів

державної влади з вимогою обов'язкового впровадження національної мови.

Отже, сукупність засобів, які призначені на боротьбу зі стереотипним образом України, всебічно сприяють формуванню позитивного іміджу нашої держави. В умовах гібридної війни саме цей аспект державної політики грає одну з найважливіших ролей, адже служить поштовхом для зміцнення позицій країни на міжнародній арені, а також відіграє не менш значиму роль у процесі творення суспільної думки на користь України.

Література

1. Всеукраїнський форум «Україна 30». – [Електронний ресурс]. – Режим доступу:https://ukraine30.com/.

2. ГЕННАДІЙ МАКСАК Просування іміджу України за кордоном. – [Електронний ресурс]. – Режим доступу:http://fpp.com.ua/topic/prosuvannya-imidzhu-ukrayiny-za-kordonom/.

3. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». – [Електронний ресурс]. – Режим доступу:https://www.president.gov.ua/documents/472017-21374.

4. Ukraine NOW Новий брендинг України. – [Електронний ресурс]. – Режим доступу: https://banda.agency/ukrainenow/.

УДК 351.86

Воробчук К.М.
Шепета О.В.
кандидат юридичних наук, доцент,
Національна академія Служби безпеки України

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

У період соціального та збройного конфлікту в Україні надзвичайно актуальними є проблеми забезпечення ефективної протидії викликам та загрозам інформаційній безпеці. Це пов'язано з тим, що сучасна боротьба держави за свою незалежність – це особлива консолідована діяльність не тільки суб'єктів забезпечення інформаційної безпеки, а й суб'єктів які беруть безпосередню участь у захисті державного суверенітету, територіальної цілісності, антитерористичних операціях, а також нормотворчих органів державної влади, науковців і засобів масової інформації.

Аналіз інформаційного простору дає підстави стверджувати, що з початком анексії Криму та воєнних дій на Сході країни спостерігалися нові форми прояву інформаційного протиборства. У наслідок несформованої за

часи незалежності дієвої системи забезпечення інформаційної безпеки, Україна стикнулася з низкою загроз в усіх сферах національної безпеки, що в свою чергу вплинули на розпалення міжнаціональної ворожнечі, сепаратистські настрої, посягання на державний суверенітет і територіальну цілісність України. Відповідно держава була не готова до оперативного створення «інформаційної броні».

Як в мирний, так і військовий час досягнення інформаційної переваги над вірогідним, потенційним або реальним противником стає однією з основних цілей провідних країн світу, і в першу чергу для України. Основним інструментом для досягнення відповідної переваги над противником є спеціальні інформаційні операції.

У сучасних умовах безперервний розвиток техніки сприяє послідовному підвищенню обсягу і швидкості поширення інформації. Удосконалюються можливості інформаційного охоплення великих територій та мас людей у найкоротші терміни. Передусім це стосується сфери інформаційної безпеки та інформаційного протиборства.

Основним засобом ведення інформаційного протиборства є національні й транснаціональні ЗМІ, а також будь-які інші інформаційні мережі, здатні впливати як на світогляд, політичні погляди, правосвідомість, менталітет, духовні ідеали та ціннісні установки окремої людини, так і на суспільство в цілому.

Комплекс заходів, який у XX столітті отримав назву СІО, ще з незапам'ятних часів супроводжував бойові дії.

Ще в IV ст. до н. е. з'явилась перша фундаментальна праця блискучого китайського стратега й мислителя Сунь-Цзи "Мистецтво війни", в якій було написано: "Засобом, завдяки якому освічені правителі та мудрі полководці виступали і підкоряли інших, а їхні досягнення мали перевагу над багатьма, було попереднє знання. Попереднє знання не можна отримати від демонів та духів, не можна одержати з явищ або небесних знамень; воно має бути отримане від людей, які знають справжній стан противника".

Кожна інформаційна війна має свої наслідки, і Україна в цьому плані не виняток. За той час, що проводиться інформаційна війна на Україну, ми, як країна, зазнали наступні втрати: 1) збільшення еміграції населення; 2) втрата частини території (анексія Криму, окупація частини Донецької і Луганської областей); 3) спад промислового виробництва. І якщо при звичайній війні приходять до бажаного результату через залякування і знищення, то в інформаційній війні все робиться багато в чому через маніпуляцію свідомістю і громадською думкою. З урахуванням цих чинників інформаційний розвиток України має здійснюватися в рамках системної та збалансованої державної політики, здатної забезпечити захист суспільства, держави і громадян від інформаційно-психологічної експансії суб'єктів геополітичної конкуренції.

Література

1. Історія інформаційно-психологічного протиборства : підруч. / [Я.М.Жарков, Л.Ф.Компанцева, В.В.Остроухов В.М.Петрик, М.М.Присяжнюк, Є.Д.Скулиш] ; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д.Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2012. – 212 с.
2. ВСТУ 01.004.004 – 2014 (1). Воєнна політика, безпека та стратегіччне планування. Інформаційна безпека держави у воєнній сфері. Терміни та визначення. – Вид. Збройні сили України. – Київ, 2014. – 22 с.
3. «Юстініан. Юридичний журнал» : М. Галамба. Сутність, види та методи спеціальних інформаційних операцій [Електронний ресурс] – Режим доступу : http://www.justinian.com.ua/article.php?id=2524.
4. Литвиненко О. В. Спеціальні інформаційні операції та пропагандистські кампанії :монографія / О. В. Литвиненко. – К. : ВКФ “Сатсанга”, 2000.
5. Сунь-Цзи “Мистецтво війни” ВСЛ.2015.

УДК 351

Гаврилюк Я.М.
Національна академія Служби безпеки України

АНАЛІЗ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Сьогодні актуальним завданням для України є моніторинг загроз інформаційній безпеці для реалізації інформаційної політики, спрямованої на забезпечення національних інтересів. Національний інформаційний простір являє собою сферу інформаційних обмінів щодо створення нової інформації, її захисту та використання.

Проаналізувавши відповідність політики держави щодо забезпечення інформаційної безпеки України приведемо матрицю SWOT-аналізу сучасного стану зовнішнього та внутрішнього безпекових середовищ в сфері інформаційної безпеки України:

Сильні сторони

1. Потужний науковий потенціал у сфері інформатизації та зв’язку.
2. Велика кількість провайдерів зв’язку, магістральних оптоволоконних ліній зв’язку.
3. Висока прибутковість та привабливість телекомунікаційної галузі.
4. Інформативний супротив інститутами громадянського суспільства України деструктивним інформаційним впливам.
5. Створення головного органу контрпропаганди – Міністерства інформаційної політики України.

Слабкі сторони

1. Низька на світовому ринку конкурентна спроможність національної інформаційної продукції.

2. Недостатній рівень розвитку вітчизняної інформаційної інфраструктури.

3. Недосконалий захист інформації від несанкціонованого доступу в результаті використання іноземної техніки та інформацій технологій.

4. Технологічна залежность держави від іноземних інформаційно-комунікаційних технологій.

5. Недостатнє інформаційне покриття на окупованих територіях України.

6. Недосконала нормативно-правова база з питань забезпечення інформаційної безпеки.

7. Відсутня інтегрованість в єдину систему міжнародної інформаційної безпеки.

Можливості

1. Стимулювання конкурентоспроможного виробництва національного інформаційного продукту та введення новітніх інформаційних технологій.

2. Забезпечення ефективної безпеки інформаційно-телекомунікаційних систем, які працюють в інтересах управління країною, забезпечують потреби безпеки та оборони держави, усіх сфер економіки, систем управління всіма об'єктами критичної інфраструктури.

4. Створення та впровадження національної системи кібербезпеки і нормативно-законодавчої бази її забезпечення.

5. Створення та впровадження систем швидкого реагування інформаційним атакам, спецпідрозділів сектору безпеки для ведення інформаційно-психологічних операцій.

Загрози

1. Поширення недостовірної, упередженої та спотвореної інформації в зарубіжному інформаційному просторі, що завдає прямої шкоди національним інтересам держави.

2. Загроза безпечному та стабільному функціонуванню національних інформаційно-технологічних систем від проявів кібернетичної злочинності та кібернетичного тероризму.

3. Негативні інформаційні впливи, які спрямовані на підрив суверенітету, конституційного ладу, недоторканості кордонів і територіальної цілісності України.

4. Порушення регламенту збирання, зберігання, обробки та передачі інформації з обмеженим доступом на підприємствах оборонно-промислового комплексу держави, органах військового управління, в сфері національної економіки.

6. Незахищеність персональних даних громадян держави та електронних баз даних.

У вищенаведеній матриці SWOT-аналізу вказана реальна оцінка стратегічного стану України в сфері забезпечення інформаційної безпеки.

Сильні сторони держави трансформують зовнішні можливості у реальні, підвищуючи ймовірність їх реалізації. Держава повинна перетворювати загрози працюючи над слабкими сторонами і реалізувавши необхідні стратегічні кроки на придатні стратегічні альтернативи.

Таким чином, щоб досягнути певного рівня безпеки інформації в Україні, необхідно сформувати єдиний механізм забезпечення інформаційної безпеки держави на основі вирішення наступних питань:

- створити системи нормативно-правових актів, які регулюватимуть відносини в області забезпечення інформаційної безпеки;
- організувати безпосередню діяльність державних органів влади і недержавних організацій стосовно забезпечення інформаційної безпеки держави, суспільства і особистості, а також через інтереси ефективно управляти цією діяльністю;
- побудувати системи забезпечення інформаційної безпеки України на основі головних принципів забезпечення безпеки;
- розробити механізм вироблення політичних рішень, їх виконання та контролю.

Література

1. Богуш В. Інформаційна безпека держави/ В. Богуш, О. Юдін // – К.: «МК-Прес», 2017. – 432 с.

2. Про Міністерство: Міністерство інформаційної політики України [Електронний ресурс]. – Режим доступу : https://mip.gov.ua/content/pro-ministerstvo.html?PrintVersion.

УДК 32:351:316.42

Гайдай В.І.
Національна академія державного управління
при Президентові України

НАПОВНЕННЯ МІСЦЕВИХ БЮДЖЕТІВ: ІНФОРМАЦІЙНА СКЛАДОВА

З квітня 2014 року відбувається Реформа децентралізації влади в Україні.

Суть реформи децентралізації зводиться до передачі повноважень та фінансів від державної влади - органам місцевого самоврядування, для якнайкращого задоволення кожного мешканця населеного пункту у реалізації права на доступну, сучасну, якісну медицину й освіту, доступні та якісні адміністративні, комунальні, соціальні послуги, на вплив на прийняття рішень щодо забезпеченням гарними дорогами, вивіз сміття та освітлення вулиць. Ідея полягає в тому, щоб люди могли впливати на якість цих послуг через наближення людей до органів та осіб які надають відповідні послуги.

Логічним є те, що найближчою до людей владою є органи місцевого самоврядування: сільські, селищні міські ради та їхні виконкоми. Отже саме вони повинні мати не тільки широкі повноваження а і інформацію про нагальну необхідність людей щодо потреб, бажань, мати необхідні навички та вміння для задоволення потреб, важливим є розуміння взаємозалежності населення та органів влади, щодо наповнення бюджету та витрачання коштів бюджету, та нести відповідальність один перед одним.

Станом на 2021 рік реформа децентралізації має реальні здобутки, серед яких виділимо найголовніші:

- прийнято зміни до Бюджетного та Податкового кодексів України, завдяки яким відбулася фінансова децентралізація, місцеві бюджети зросли на 219,7 млрд грн: з 70,2 млрд. в 2014 до 289,9 млрд.грн. в 2020 році (без урахування міжбюджетних трансфертів). [1]

- створено 1469 об'єднаних територіальних громад (ОТГ). До складу цих ОТГ увійшли більше 4487 колишніх місцевих рад. 11 млн. людей проживають в ОТГ. Отримано у комунальну власність майже 1,5 млн.га. земель сільськогосподарського призначення за межами населених пунктів;

- прийнято закон «Про співробітництво територіальних громад», який створив механізм вирішення спільних проблем громад: утилізація та переробка сміття, розвиток спільної інфраструктури тощо. Для продовження реформи готуються законопроекти, зокрема: «Про службу в органах місцевого самоврядування» (нова редакція) який покликаний підвищити престижність служби в ОМС, збільшити мотивацію місцевих службовців до розвитку громад та власного розвитку, готується законопроект щодо державного нагляду за законністю рішень органів місцевого самоврядування, та «Про місцевий референдум».

Проте, незважаючи на здобутки децентралізації влади, серед яких значна частка полягає у прийнятті нормативно-правових актах, невирішеною є проблема взаєморозуміння органів влади та мешканців - платників податків у відповідальності щодо виконання кожним обов'язків щодо наповнення бюджету – мешканцями, та створення умов для наповнення та витрачанням коштів – органами місцевого самоврядування для виключного для задоволення потреб населення.

Так, за результатами дослідження української економіки компанії Ernst & Young у рамках укладеного Меморандуму про співробітництво з Міністерством розвитку економіки, торгівлі та сільського господарства України, Національним банком України та Державною службою статистики України, 846 млрд гривень або 23,8% від офіційного ВВП за 2018 рік, перебуває в тіні [2].

Та враховуючи, що лідером недовіри є державний апарат загалом (йому і посадовцям не довіряють 78% респондентів), що свідчить про високий рівень відчуження між структурами влади і суспільством, що зумовлює негативну оцінку громадянами діяльності влади [3].

Можна дійти висновку, що реформа децентралізації попри значні здобутки, користується певною недовірою та нерозумінням у громадян, адже була започаткована, саме, органами державної влади, та існує взаємозалежність між довірою до влади та рівнем добровільної сплати податків платниками, адже частина сплачених податків зараховується до бюджетів ОМС.

Відповідно, враховуючи що ОМС діють в безпосередній близькості з громадянами для вирішення їх проблем та для забезпечення їх життєдіяльності, необхідно постійно висвітлювати інформацію про діяльність ОМС як про здобутки так і про наявні можливості, як про недоліки в роботі так і про упущену вигоду, тобто надавати інформацію про діяльність виборних осіб ОМС (Голову ОМС, депутатів місцевої ради) про їх дії та бездіяльність для забезпечення об'єктивною інформацією виборців для збільшення довіри мешканців та покращення добровільної сплати податків, надавати інформацію про взаємозалежність між сплатою податків, які сплачуються на задоволення потреб платника, та збільшенням рівня задоволення потреб кожного мешканця, тобто проводити роз'яснювальну роботу, що саме мешканці населеного пункту, через сплачені податки, оплачують роботу посадових осіб ОМС, а посадові особи найняті платниками податків для ефективного задоволення реальних потреб населення.

Література

1. Офіційний сайт Міністерства фінансів України [Електронний ресурс].- Режим доступу: https://mof.gov.ua/uk.

2. Офіційний сайт Національного банку України [Електронний ресурс].- Режим доступу: https://bank.gov.ua/ua/news/all/doslidjennya-tinovoyi-ekonomiki-v-ukrayini--mayje-chvert-vvp--abo-846-mlrd-griven--perebuvaye-v-tini.

3. Офіційний сайт Українського центру економічних та політичних досліджень ім. О. Разумкова [Електронний ресурс].- Режим доступу: https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/pochatok-novogo-politychnogo-roku-dovira-do-sotsialnykh-instytutiv-lypen-2020r.

УДК 355.451:004.7

Гальчинський Л.Ю.
кандидат технічних наук, доцент
Горобець А. М.
Національний технічний університет України
«КПІ імені Ігоря Сікорського»

ОЦІНЮВАННЯ РІВНЯ СПРОМОЖНОСТІ ПЕРСОНАЛУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДО ЗАХИСТУ ВІД КІБЕРЗАГРОЗ

Науково-технічний прогрес стрімко породжує зростання нових можливостей у всіх сферах діяльності, зокрема і сфері промислових технологій.

Проте нові технології приносять з собою і нові ризики: промислові об'єкти все частіше піддаються кібератакам. За останнє десятиліття кібербезпека в середовищах систем управління в промисловості (Industrial Control Systems- ICS) все більше стає питанням національної безпеки. Тенденція до зближення інформаційних технологій та технологій експлуатації тепер означає, що організації, що охоплюють широкий спектр промислових об'єктів, серед яких є і об'єкти критичної інфраструктури, залежать від IT-інфраструктури та технологій. Це також означає, що ці організаційні платформи мають чисельні вразливості та сприйнятливі до кібератак. Всім добре відомо, що інформаційна технологія захисту від кіберзагроз постійно вдосконалюється. У відповідь на нові кіберзагрози з'являються відповідні засоби боротьби з ними. Однак навіть найбільш досконалі інформаційні технології кіберзахисту не можуть вирішити проблему кіберзахисту в цілому. Питання у тому, що середовище промислової системи управління відноситься до області, де виконуються операції та процеси промислового контролю. ICS - це система промислових технологій та інфраструктур, побудована та експлуатована людьми (персоналом) для виконання процесів досягнення цільових продуктів або послуг. Це означає, що технологія захисту (апаратне та/або програмне забезпечення) вирішує лише частину більшої проблеми безпеки. Технологія часто є настільки ж слабкою та вразливою, як і люди, які розробляють або експлуатують її, а також процеси, розроблені та структуровані для її використання. Людський фактор настільки ж важливий, як і технічні фактори безпеки ICS. Реальні інциденти останніх років також підтверджують цю точку зору. Протягом останніх років повідомлення ЗМІ демонструють тривожне зростання кіберзагроз та атак на ICS у всьому світі.

У Німеччині в 2014 році на тепловій електростанції п'ятнадцятирічний підліток зі свого комп'ютера підключився до мікроконтролерів, які були доступні до мережі сервісного центру. Керуючи тепловою станцією, він викликав аварійну зупинку обладнання. Найгучніша кібератака на об'єкт атомної енергетики сталася в 2013 році. Вірус Stuxnet проник в систему управління центрифугами на заводі зі збагачення урану в Ірані, зіпсувавши близько третину з них. Зловмисники, не маючи доступу до мережі, застосували техніку атаки із зараженим USB-накопичувачем на сторонню організацію технічного обслуговування. У 2015 році на Україні зловмисники перехопили управління електричними мережами і відключили кілька областей. Системи операторів електромереж були заблоковані: ті бачили, як відбувалося відключення, але не могли йому перешкодити. Атака на енергомережу України була повторена у 2016 році. У червні 2017 року масштабній атаці було піддано мережі цілого ряду державних та приватних установ, зокрема офіс компанії «ЕНЕРГОАТОМ». Вразливою виявилась корисна система бухгалтерського обліку M.E.Doc. Одним із способів визначення кібербезпеки є гармонізація можливостей людей, процесів та (або) технологій;

захищати та контролювати як санкціонований, так і/або незаконний доступ, знищення або модифікацію електронних обчислювальних систем, даних та інформації, яку вони мають. Однак більшість сучасних рішень щодо безпеки мають технологічний характер. Контексти та вимоги безпеки людей та процесів часто не враховуються, що нерідко призводить до однобічної безпеки, яку злочинно експлуатують злісні хакери.

На наш погляд фундаментальною основою для підсилення безпеки об'єктів критичної інфраструктури взагалі та про кібербезпеку зокрема мав би стати Закон України "Про критичну інфраструктуру та її захист" поданий ще у квітні 2019 року і досі ще не прийнятий Верховною Радою. Стаття 34 Проекту цього Закону передбачає, що контроль за рівнем безпеки об'єктів критичної інфраструктури здійснюється шляхом оцінки захищеності об'єктів критичної інфраструктури, причому проведення контролю визначається Кабінетом Міністрів України за поданням Уповноваженого органу у сфері захисту критичної інфраструктури України. Про методику оцінки захищеності об'єктів нічого не сказано. Можливо, це і недоцільно, проте такі методики мають бути для об'єктивного оцінювання рівня захищеності, в тому числі і методика оцінки кіберзахищеності. Причому ця методика має передбачати оцінку як технологічної складової, так і оцінку рівня готовності персоналу об'єктів критичної інфраструктури до кіберзагроз. Очевидно, що така методика має носити кількісний характер оцінювання і її розробка потребує додаткових досліджень, які в Україні ще не проводились. На наш погляд доцільно використати зарубіжний досвід. Так деяких публікаціях [2]-[3] викладається ідея кількісного оцінювання персоналу середовища ICS на основі моделі, яка ґрунтується на тестуванні персоналу за спеціальною технологією. Цей підхід до оцінки доповнює традиційні технічні можливості та аналіз вразливості. Підхід та заходи можуть бути корисними для аудиторів безпеки, аналітиків, менеджерів об'єктів критичної інфраструктури при проведенні оцінок загроз та вразливостей на рівні людини, виявленні найбільш вразливих людських агентів, а також областей, де рівень безпеки низький. Приймаючи відповідні рішення на основі об'єктивних оцінок, можна суттєво вплинути на поліпшення загальної організаційної безпеки.

Література

1. David Kushner, "The Real Story of Stuxnet". IEEE Spectrum, March 2013, http://spectrum.ieee.org/telecom/internet/the-autistic-hacker/0 .

2. Human factor security: evaluating the cybersecurity capacity of the industrial workforce Ani, Uchenna Daniel; He, Hongmei; Tiwari, Ashutosh Journal of Systems and Information Technology, Volume 21, Number 1, 2019, pp. 2-35(34).

3. DaVeiga,A.andEloff,J.H.P.(2010) "A framework and assessment in strument for Information Security Culture",Computers &Security, Vol.29, No.2010, pp.196207.

УДК 351.86:659.3/.4:004](477)
Горбатюк П.М.
Національна академія державного управління
при Президентові України

НАПРЯМИ ЗАБЕЗПЕЧЕННЯ ГРОМАДСЬКОГО ПОРЯДКУ ОРГАНАМИ СЕКТОРУ БЕЗПЕКИ УКРАЇНИ

Згідно Закону «Про національну безпеку України, громадська безпека і порядок - захищеність життєво важливих для суспільства та особи інтересів, прав і свобод людини і громадянина, забезпечення яких є пріоритетним завданням діяльності сил безпеки, інших державних органів, органів місцевого самоврядування, їх посадових осіб та громадськості, які здійснюють узгоджені заходи щодо реалізації і захисту національних інтересів від впливу загроз [2].

Беручи до уваги нинішню ситуацію із станом законності і правопорядку в Україні, невщухаючу гібридну агресію з боку Російської Федерації, необхідність підтримання на належному рівні громадської безпеки в нашій державі виступає одним із пріоритетів забезпечення національної безпеки в цілому, безпосередньо впливаючи на процеси у соціальноекономічній, політичній, морально-психологічній та інших сферах життєдіяльності українського суспільства [1].

Головним напрямом забезпечення громадського порядку органами сектору безпеки України є посилення ролі цих органів як гарантів безпеки особистості і прав власності, вдосконалення правового регулювання попередження злочинності (в тому числі в інформаційній сфері), корупції, тероризму та екстремізму, поширення наркотиків і боротьби з такими явищами, а також розвиток взаємодії органів сектору безпеки з громадянським суспільством, підвищення довіри громадян до правоохоронної систем України, ефективності захисту прав і законних інтересів українських громадян.

Підтримка правопорядку в сучасних умовах багато в чому залежить від ефективності взаємодії регіональних органів виконавчої влади та правоохоронних органів щодо профілактики правопорушень, яка у великій мірі базується на використанні інформаційних механізмів у процесі такої взаємодії. Рівень правопорядку в регіоні впливає на формування оцінки громадянами діяльності не тільки правоохоронних органів, а й органів виконавчої влади. Підвищення рівня правопорядку сприяє соціально-економічному розвитку регіону та підвищення його інвестиційної привабливості.

Інформаційною складовою пріоритетних напрямів забезпечення громадського порядку органами сектору безпеки України можна назвати:

- придбання оперативно-технічних і спеціальних технічних засобів контролю і зв’язку, електронної обчислювальної та копіювальної техніки,

призначених для виконання завдань з охорони громадського порядку, забезпечення громадської безпеки;

- розвиток систем відеоспостереження в найбільш криміногенних місцях і місцях масового перебування людей;

- комунікативна компанія щодо заохочення добровільної здачі населенням незаконно зберігається зброї, боєприпасів і вибухових речовин;

- підготовка та розміщення в засобах масової інформації соціальних радіороликів і відеороликів, програм з профілактики злочинів і терористичних актів, залученню громадян до правоохоронної діяльності, пошуку зниклих без вести;

- виготовлення засобів наочної агітації (пам'яток, буклетів, інформаційних листків та ін.) правоохоронної спрямованості, присвячених боротьбі з тероризмом і екстремізмом;

- проведення суспільно-політичних і просвітницьких заходів, навчальної та аналітичної роботи з метою профілактики правопорушень, екстремізму і тероризму.

Література

1. Концептуальні підходи щодо забезпечення громадської безпеки: іноземний досвід, висновки для України. URL: http://old2.niss.gov.ua/content/articles/files/1_Siomin-8f832.pdf.

2. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VII. Відомості Верховної Ради (ВВР). 2018. № 31. Ст.241 URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

УДК 004.56.5

Гук О.М.
Національний університет оборони України
імені Івана Черняховського

ЗАХИСТ ІНФОРМАЦІЇ В ДЕРЖАВНИХ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ В УМОВАХ КІБЕРВПЛИВУ ПРОТИВНИКА

В сучасних умовах, державні інформаційні ресурси, відомчі (у т.ч. інформаційні системи ЗС України) та звичайні користувачі є критично залежними від Інтернету, інформаційно-телекомунікаційних систем та інформаційних технологій. Як наслідок, важливу роль має неперервність функціонування життєво важливих систем електроживлення і зв'язку, впевненість в тому, що послуги (сервіси) звязку, інформаційний обмін між абоне-

нтами будуть забезпечні на необхідному рівні. При цьому більшість мережних систем та інфраструктур виявляються дуже вразливими, чим вміло користуються кіберзлочинці.

Аналіз функціонування інформаційно-телекомунікаційних систем воєнного призначення показав, що відомі властивості складних технічних систем, такі як стійкість, надійність, живучість, відмовостійкість характеризують функціонування систем при впливі відмов та пошкоджень, але не дозволяють в повному обсязі описати процеси функціонування цих систем в умовах кібервпливу противника.

Зазначена властивість характеризує здатність системи долати нештатні ситуації (інциденти), що виникають в наслідок деструктивного впливу противника. Властивість функціональної стійкості інформаційно-телекомунікаційних систем необхідно розглядати, як можливість зберегти її працездатність при певному числі відмов та дестабілізуючих впливів, до яких можна віднести кібервплив противника.

На погляд автора кібервплив – це процес впливу на визначені елементи кіберпростору з метою порушення процесів управління в кібернетичних системах противника шляхом зміни нормальних режимів їх функціонування. Об’єктами кібервпливу можуть виступати: органи управління, комп’ютерні системи і мережі; системи зв’язку та автоматизовані системи управління; управляючі елементи систем озброєння, військової техніки, критичних об’єктів інфраструктури; програмне забезпечення, бази даних тощо.

Системи захисту в розподілених системах можна розділити на дві незалежні частини. Одна з них – це зв’язок між користувачами або процесами, можливо, розташованими на різних машинах. Принциповий спосіб гарантувати захист взаємодії – це захищений канал.

Інша частина систем захисту – це авторизація, яка дозволяє гарантувати, що процеси отримають тільки ті можливості доступу до ресурсів розподіленої системи, на які мають право. Авторизацію і контроль доступу можна розглядати спільно. У поєднанні з традиційними механізмами контролю доступу, також необхідно враховувати контроль доступу при роботі з мобільним кодом, наприклад з агентами.

Захищені канали та засоби контролю доступу потребують механізмів для роботи з криптографічними ключами, а також механізмів додавання користувачів в систему і видалення їх з неї. В цьому полягає управлінням захистом. Необхідно постійно вирішувати питання, пов’язані з управлінням криптографічними ключами, управлінням захистом в групах і обробкою сертифікатів, що засвідчують право власника на доступ до певних ресурсів.

Державні розподілені інформаційні системи постійно знаходяться в умовах відсутності повної інформаційної безпеки (кібербезпеки), що вказує на необхідність вироблення загального дисциплінованого підходу до

управління ризиками в кіберпросторі та визначення основних пріоритетів щодо захисту інформації вцілому.

Належне функціонування інформаційно-телекомунікаційних систем в умовах кібервпливу противника забезпечить ефективність управління своїми силами і засобами, та надасть перевагу в умовах сучасного протиборства.

Література

1. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” документ 80/94-ВР, чинний, поточна редакція – Редакція від 04.07.2020, підстава - 681-IX.

2. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков / Видавнича група BHV, 2009. – 608 с.: іл.

3. Гук О.М. Проблематика захисту інформації в розподілених інформаційних системах військового призначення / О.М.Гук //Застосування Сухопутних військ Збройних Сил України у конфліктах сучасності: Збірник тез доповідей науково-практичної конференції. – Львів: НАСВ, 2020. – 268 с.

4. Гук О.М. Дії в кіберпросторі під час підготовки та ведення мережецентричної війни / О.М.Гук, О.Ю. Чередниченко, Р. М. Штонда., І.О.Диба // Сучасні інформаційні технології у сфері безпеки та оборони. - 2017. - № 2. - С. 107-111.

УДК 327.5:316.776.23

Даценко А.Ю.
Національний інститут стратегічних досліджень

ЩОДО ОЦІНКИ ЕФЕКТИВНОСТІ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА ПРОПАГАНДІ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

Протистояти сучасній російській пропаганді та дезінформації, яка має потужний потенціал ефективності завдяки своїм характерним властивостям (великий обсяг пропагандистських повідомлень, використання безлічі каналів для їх трансляції; швидкість й безперервність подачі матеріалу та його повторення; відсутність висвітлення об’єктивної реальності; відсутність логіки й послідовності), є досить нетривіальним завданням.

На погляд фахівців у сфері інформаційного протиборства, у даному випадку традиційні способи боротьби із пропагандою малоефективні, оскільки переваги, які отримує російська пропаганда внаслідок можливості запропонувати аудиторії свою версію подій першою (дискредитація її після першого отриманого аудиторією враження вимагає вже набагато більше зусиль), можуть бути нівельовані тільки за умови, якщо у першу чергу аудиторія буде отримувати правдиву інформацію. Але допоки професійні й правдиві журналісти перевірять факти, маховик пропаганди вже розкрутиться на повну потужність, адже фабрикація «фактів» займає набагато менше

часу, аніж їх перевірка. До того ж, спростування й надання правдивих версій подій «поверх попереднього вимислу» не дає бажаного психологічного результату, бо, якщо вже пройшов значний проміжок часу, людині буде вже складно згадати, що з почутого/побаченого правда, а що ні [1].

Усі ці обставини мають бути обов'язково врахованими у процесі протидії дезінформації та ворожій пропаганді. Йдеться зокрема про заходи, що впроваджуються країнами ЄС та США , а також останнім часом нашою країною (цьогорічне зупинення мовлення трьох проросійських телеканалів, запуск роботи Центру протидії дезінформації при РНБО України, тощо).

Доведено зокрема, що ефективність спростувань і нових версій підвищується під впливом трьох чинників: (1) попередження деструктивного інформаційно-психологічного впливу уже в процесі первинного поширення/впливу дезінформації; (2) повторення спростувань та нових правдивих версій; (3) виправлення, які допомагають створити альтернативні версії подій, що заповнюють пробіли в їхньому розумінні, коли уже усунуті вигадані (спростовані) «факти». Попередження щодо подібних «фактів» навіть більш ефективні, ніж їх спростування чи нові версії подій, запропоновані в порядку інтерпретації пропаганди. Проте, найбільш дієвим засобом у боротьбі з російською пропагандою іноземними дослідниками вважається наступальна контрпропаганда: «Якщо російська пропаганда націлена на досягнення певних цілей, то за допомогою контрпропаганди можна запобігти небажаному розвитку подій, або звести до мінімуму ефект від досягнення ними своїх цілей» [2].

Ключовим завданням контрпропагандистської роботи з російською цільовою аудиторією є створення таких наративів і підбір таких каналів їхнього донесення до аудиторії, які уможливлять сприйняття цих наративів цільовою аудиторією. Інакше кажучи, важливо прорвати «інформаційну оболонку» (захисну блокаду), донести інформацію у бажаній інтерпретації до людей – «лідерів думок», які зможуть вплинути на погляди, цінності й установки цільової аудиторії. Саме тому цільовим завданням контрпропаганди є прорив інформаційної монополії ЗМІ РФ у їхньому мовленні на певні сегменти населення.

Для цього, насамперед, необхідно доносити власні наративи зрозумілою та прийнятою в цій аудиторії мовою й використовувати відповідні образи. Водночас, не можна не погодитися з фахівцями, що найбільш радикальних прихильників «руського міра», ідеологів російського імперіалізму навряд чи вдасться переконати за допомогою подібних наративів. Однак на пересічних громадян Росії, що поділяють на якомусь проміжкові часу неоімперську ідеологію, можна й потрібно спробувати вплинути, відвернути їх від цієї ідеології.

У даному контексті науковцями пропонується концепція «когнітивної інфільтрації» («cognitive infiltration») для креативного вирішення способу

руйнування «інформаційної оболонки» і донесення власних наративів до цільової аудиторії. Суть запропонованої концепції полягає в інформаційному проникненні (інфільтрації) у замкнуту інформаційну оболонку з метою доведення альтернативної інформації, що підриває «ідейний моноліт» і сіє сумніви серед пересічних громадян відносно теорій, переконань і фактів, які циркулюють в їх середовищі, шляхом внесення «когнітивного розмаїття», тобто через чутки, перекази, анекдоти, епіграми, тощо [3].

Разом з тим, проблему донесення інформації до цільової аудиторії Росії не слід спрощувати. Способів донесення такої інформації не дуже багато із-за наявної замкнутої «інформаційної оболонки», створеної навколо населення РФ пропагандистськими ЗМІ. Найбільш доступними є наступні способи й механізми:

- демонстрація на міжнародних майданчиках у ході науково-представницьких заходів (конференцій, форумів, "круглих столів", тощо);
- поширення через супутникове телебачення;
- розміщення в російському сегменті мережі Інтернет включно із Інтернет-сайтами, соціальними мережами й блогами;
- розсилка повідомлень та спілкування через мобільний зв’язок.

За висновками фахівців, через обмежені можливості України доцільно активно задіяти, передусім, якісні Інтернет-ресурси: високопрофесійні портали й сайти, які відрізняються привабливістю інфографіки, оперативністю оновлення, швидкою реакцією на останні події в регіонах і у світі, продуманістю інтерфейсу, адресною орієнтацією на різні соціальні групи людей різного віку.

Література

1. Lewandowsky, Stephan, Ullrich K. H. Ecker, Colleen M. Seifert, Norbert Schwarz, and John Cook, “Misinformation and Its Correction: Continued Influence and Successful Debiasing,” Psychological Science in the Public Interest, Vol. 13, No. 3, December 2012, pp. 106–131.

2. Paul, Christopher. Matthews, Miriam. The Russian “Firehose of Falsehood” Propaganda Model / Christopher Paul, Miriam Matthews [Електронний ресурс]. Режим доступу: https://www.rand.org/pubs/perspectives/PE198.html (дата звернення 18.03.2021).

3. Почепцов Г. Анекдоты и слухи при переходе от книжного мира в мир интернета [Електронний ресурс]. Режим доступу: https://ms.detector.media/mediaanalitika/post/15672/2016-01-17-anekdoty-y-slukhy-pry-perekhode-ot-knyzhnogo-myra-v-myr-ynterneta/ (дата звернення 18.03.2021).

УДК 691.392
Дяченко С.А.
Національний університет оборони України
імені Івана Черняховського

АКТУАЛЬНІСТЬ РОЗРОБКИ МЕТОДИКИ АДАПТИВНОГО УПРАВЛІННЯ ПАРАМЕТРАМИ ВІЙСЬКОВИХ РАДІОМЕРЕЖ

На даний час відбувається побудова єдиного глобального інформаційного простору між елементами систем управління різноманітного призначення.

Головними відмінностями цієї архітектури є використання систем високого рівня інтеграції на основі принципів побудови мережі Інтернет.

З цією метою здійснюється перехід від різнотипних незалежно функціонуючих підсистем до інтегрованих систем зв'язку та передачі даних (ІСЗ ПД). Це, в свою чергу, вимагає використання багатофункціональних радіозасобів, які дозволяють здійснювати наскрізне управління параметрами систем військового радіозв'язку.

Багатофункціональність радіостанцій реалізується за рахунок використання широкого класу сигналів, способів кодування, заходів підвищення завадозахищеності, режимів передачі інформації, алгоритмів вибору раціональної топології та маршруту передачі інформації [1; 2].

Проблема сумісності засобів радіозв'язку різних стандартів і діапазонів у теперішній час для тактичної ланки управління збройних сил провідних країн світу реалізується шляхом використання технологій програмованих радіостанцій (software defined radio, SDR) та програмованих мереж (Software-defined Networking, SDN).

Властивість засобів зв'язку змінювати свої основні технічні характеристики шляхом перепрограмування дозволяє проводити управління як канальними, так і мережевими ресурсами.

Ключовою особливістю ведення сучасних військових операції (бойових дій) є функціонування в умовах апріорної невизначеності щодо стану радіоелектронної обстановки. Зазначене обумовлюється динамічною зміною топології мережі внаслідок переміщення засобів радіозв'язку, фізичним знищенням радіозасобів, зміни підстилаючої поверхні та радіоелектронного подавлення.

Враховуючи зазначене, постає необхідність у розробці методики управління канальними та мережевими ресурсами військових радіомереж в умовах невизначеності радіоелектронної обстановки.

Проведений аналіз робіт [2-6] дозволяє стверджувати про те, що існуючі наукові здобутки не дозволяють проводити наскрізне управління канальними та мережевими ресурсами військових мереж радіозв'язку, а лише проводять окремі управляючі впливи на окремо взятому рівні моделі взаємодії відкритих систем. Все це не дозволяє ефективно використовувати на-

явний радіоресурс військових радіомереж та комплексно протидіяти дестабілізуючим факторам, що впливають на ефективність функціонування військових радіомереж.

Отже для підвищення ефективність функціонування військових радіомереж необхідно проводити комплексне управління параметрами військових радіомереж на канальному та мережевому рівнях моделі взаємодії відкритих систем. Зазначене можливо досягти шляхом розробки відповідних процедур управління, які дозволять: на канальному рівні моделі OSI:

– проводити вибір робочих частот з урахуванням впливу навмисних завад та прогнозованої стратегії засобів радіоелектронної боротьби;

– визначати раціональний режим роботи засобів радіозв'язку;

на мережевому рівні моделі OSI:

– проводити вибір топології системи військового радіозв'язку;

– проводити вибір раціонального маршруту передачі інформації між елементами системи військового радіозв'язку;

– визначати розташування передавачів засобів радіозв'язку в залежності від розміщення передавачів засобів радіоелектронної боротьби;

– проводити в комплексі управління канальними та мережевими ресурсами на кожному з рівнів моделі взаємодіє відкритих мереж.

Таким чином є необхідність розробки методики адаптивного управління параметрами військових радіомереж, яка б дала змогу вирішення завдання здійснення управління на канальному та мережевому рівнях моделі взаємодії відкритих мереж.

Література

1. Шишацький А. В., Башкиров О. М., Костина О. М. Розвиток інтегрованих систем зв'язку та передачі даних для потреб Збройних Сил. // Науково-технічний журнал "Озброєння та військова техніка". 2015. No 1(5). С. 35 –40.

2. S. Kalantaievska, H. Pievtsov, O. Kuvshynov, A. Shyshatskyi, S. Yarosh, S. Gatsenko, H. Zubrytskyi, R. Zhyvotovskyi, S. Petruk and V. Zuiko. Method of integral estimation of channel state in the multiantenna radio communication systems. // Eastern-European Journal of Enterprise Technologies. Vol 5, No. 9 (95) (2018): pp 60 - 76.

3. Слюсар В. І., Зінченко А. О., Зінченко К. А. Система мобільного зв'язку стандарту GSM для потреб радіолокаційного контролю повітряного простору.// Сучасні інформаційні технології у сфері безпеки та оборони. – No 2(23). – 2015. – С. 108 - 114.

4. Слюсарь І. І., Слюсар В. І., Смоляр В. Г., Омаров М. І., Хоменко Р. В. Шляхи удосконалення систем транкінгового зв'язку України. // Новітні інформаційні системи та технології. - Полтавський національний технічний університет ім. Юрія Кондратюка, 2016. – Вип. 5. – С. 36 – 47.

5. Md. J., Piran, Quoc-Viet Pham, S. M. Riazul Islam, Sukhee Cho, Byungjun Bae, Doug Young Suh and Zhu Han. Multimedia communication over cognitive radio networks from QoS/QoE perspective: A comprehensive survey". Journal of Network and Computer Applications. 2020, pp. 1-55.

6. Majumder, T., Mishra, R. K., Singham S. S., Sahu, P. K. Robust congestion control in cognitive radio network using event-triggered sliding mode based on reaching laws. The Franklin Institute. 1-24.

УДК 338.242
Єремеєва А.М.
Тугарова О.К.
кандидат юридичних наук, доцент,
Національна академія Служби безпеки України

ЕКОНОМІЧНА СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ПАНДЕМІЇ

Сучасне забезпечення інформаційної безпеки держави в умовах COVID-19 виступає важливим детермінантом розвитку суспільства та країни. Оскільки, масштаби пандемії набули всесвітнього характеру, це значним чином відбилося на економічній парадигмі. Всі ці умови стали не тільки ударом по охороні здоров'я, але й по бізнесу, який був не готовий до таких коливань. Адже, економічний спад примусив роботодавців скоротити потреби в усіх ресурсах, в тому числі, трудових. Проте, процеси діджиталізації, які наразі формують кардинально нові вектори розвитку безперечно виступають не тільки викликами, але й пріоритетними напрямки вивчення даної сфери. А необхідність дослідження економічної складової в контексті інформаційної безпеки держави в умовах коронавірусу є актуальним питанням сучасності.

Значну увагу питанню дослідження інформаційної безпеки держави приділили такі вітчизняні вчені, як Гальчинський А., Барановський О., Єрмошенко М., Шлемко В., Мартинюк В., Пирожков С.

Своєрідність та специфічність коронавірусу виступає в тому, що катастрофічний вплив відбувся на всі сфери світової економіки. Оскільки, відбувся відтік населення по галузям, збільшився не лише офіційний рівень безробіття, але й суттєво погіршилася ситуація на, так званому, «чорному» ринку праці. Закриття кордонів, та негативні тенденції в економіках практично зупинило «колесо» розвитку.

В Україні короновірусна криза спричинила стрибкоподібне збільшення безробіття і про це свідчать вагомі статистичні дані. Зауважимо, що рівень безробіття в Україні стрімко почав зростати у квітні 2020 р., із введенням жорсткого карантину від COVID-9. Якщо у березні 2020 р. офіційно зареєстрованих безробітних в Україні було 349 000 осіб (реальний же рівень в рази більший), то уже в квітні він сягнув 457 000 осіб, у травні – 511 000 осіб, а в червні – 517 000 осіб. І лише з липня 2020 р. розпочалося скорочення – до 506 000 осіб, і в серпні – до 474 000 осіб.

Загалом же, з початку карантину в Україні статус безробітного отримали майже 432 000 осіб (станом на кінець серпня 2020 р.), що на 67 % більше, ніж за 2019 р. Безробітними стали сотні тисяч громадян: як представники інтелектуальної праці, так і найпростіших професій. На 20 серпня

2020 р. статус безробітного мали майже 488 000 українських громадян (проти 276 000 осіб у 2019 р.).

Відповідно до даних «INFO SAPINENS», карантин негативно вплинув на фінанси українців. Так, 69 % відчуло погіршення фінансового становища; 40 % українського населення планувало пережити карантин без значних фінансових втрат; 38 % відчуло негативні наслідки спалаху коронавірусу, дохід їх родин скоротився; 16 % громадян – взагалі позбулися доходу, а 14 % втратили роботу. У березні 2020 р. показник індексу очікуваної динаміки безробіття склав 168,9 %, що на 35,5 % вище за показник минулого місяця.

Важливість ситуації пояснюється тим, що на період карантину кількість користувачів соціальних мереж зросла на 9% в порівнянні з минулим, а це в свою чергу свідчить про те, що поширення дезінформації та фейків відбувається миттєво. Адже, в теперішніх умовах ери технологій, інформаційний ресурс виступає фактором впливу на конкурентоспроможність та відіграє важливу роль у забезпеченні інтересів будь-якої держави, в контексті фінансів, військового переважання, різного роду аварій, розладу системи державного управління.

Інформаційна безпека держави є однією із основоположних складових сфери національної безпеки, яка виступає на захист життєво важливих інтересів суспільства та держави. А в умовах коронавірусу збільшується кількість як внутрішніх, так і зовнішніх загроз, так званих кібератак, які можуть дестабілізувати ситуацію. Тому, критично важливо, в даних умовах забезпечити інформаційну безпеку громадянина та держави в цілому.

Узагальнюючи, зробимо висновок, що пандемія вплинула не тільки на економічну чи національну безпеку, але й залишила відбиток на кожному із нас. Цифровий простір, який функціонує в даних умовах формує завдання національній безпеці в контексті забезпечення високих показників інформаційної безпеки держави.

Література

1. Новый рынок труда: кого ищут украинские работодатели во время коронавирусного карантина. URL: https://tsn.ua/ru/coronavirus/novyy-rynok-truda-kogo-ischut-ukrainskie-rabotodateli-vo-vremya-koronavirusnogo-karantina-1530627.html.

2. Як пандемія COVID-19 змінила ринок праці в Україні. URL: https://www.ukrinform.ua/rubric-society/3104312-ak-pandemia-covid19-zminila-rinok-praci-v-ukraini.html.

3. До середини року більш як половина населення світу буде користувачами соцмереж.URL:https://www.ukrinform.ua/rubric-technology/2870117-do-seredini-roku-bils-ak-polovina-naselenna-svitu-bude-koristuvacami-socmerez.html.

4. Державна служба статистики України. URL: http:// www. ukrstat.gov.ua.

5. Державна служба зайнятості. URL: https://www.dcz.gov.ua.

УДК 355/359
Єсін О. В.
Національна академія Служби безпеки України

АНТИУКРАЇНСЬКА ІНФОРМАЦІЙНО – ПРОПАГАНДИСТСЬКА КАМПАНІЯ НА РОСІЙСЬКОМУ ТЕЛЕБАЧЕННІ

На сьогоднішній триває гібридна війна між Російською Федерацією та Україною, в якій поле битви не лише фізичний простір Донбасу, а й інформаційне середовище, саме тому дослідження пропаганди, яку здійснює Росія через свої засоби масової інформації є актуальним, потребує глибокого дослідження, адже щоб зруйнувати пропагандистську кампанію Кремля, потрібно знати що вона собою являє.

На протязі кількох років триває війна між Російською Федерацією та Україною, яка почалась з окупації Криму Росією. Відбулась дана подія не тільки за допомогою сили, а й за допомогою «правильного» настрою громадян та вдало проведених Спеціальних інформаційних операцій (СІО). Така форма ведення війни називається – не лінійна або ж «гібридна».

«Гібридна» війна — особливий тип збройного конфлікту, в якому бойовим діям відведена другорядна роль. Мета «гібридної» війни полягає у нав'язуванні противнику волі шляхом застосування різних видів сили. При цьому бойові дії відіграють допоміжну роль в ослабленні противника, будучи лише каталізатором дестабілізаційних процесів, попередньо запущених за допомогою економічних, політичних, інформаційних та інших методів. Росія була не першою державою, яка застосувала «гібридну» війну проти інших країн, а Україна — не першою жертвою «гібридної» війни [1].

Війна здійснювалась за допомогою розгортання великої інформаційної кампанії, яка включала в себе проведення великої кількості спеціальних інформаційних операцій (СІО).

СІО – це комплекс заходів інформаційно - психологічного впливу та інформаційно – технічного впливу, що здійснюються за єдиним планом з метою порушення системи державного та військового управління, впливу на морально – психологічний стан військово – політичного керівництва, населення та збройних сил визначеного об'єкта, запобігання впливу на власні сили.

Відповідно до нашого дослідження, Російська Федерація здійснює СІО за допомогою телебачення, проводячи відповідні дії для досягнення руйнівного впливу на свідомість та підсвідомість населення.

Пропаганда – являє собою поширення різних політичних, філософських, наукових, художніх, інших ідей із метою їх упровадження в громадську думку.

Відповідно до наданого визначення, ми можемо проаналізувати дії суб'єкту пропаганди, а саме дії на російському телебаченні. Метою проведення пропаганди є упровадження певних ідей, а в нашому випадку саме антиукраїнських ідей, в громадську думку, тобто населенню Росії та світовій спільноті.

Завданнями СІО та гібридної війни загалом – зниження рівня довіри до України на світовому рівні, захоплення територій, деструктивний вплив на свідомість та підсвідомість об'єктів СІО.

Визначені СІО проводяться за допомогою масштабного джерела інформації – телебачення, а саме федеральних каналів Російської Федерації, на який підготовлені особи висловлюють думку, за якою повинні слідувати особи. Для переконання суб'єктів СІО використовується перекручування інформації, надання та поширення фейків, використання не справжніх фактів. Це дає змогу здійснити вплив на свідомість та підсвідомість осіб, результатом чого є впровадження думок, які були нав'язані спікерами.

Висновки. Відповідно до дослідження дійшли висновку, що на сьогоднішній день триває гібридна війна, яка проводиться не тільки за допомогою зброї, а й за допомогою інформації. Використовуючи спеціальні інформаційні операції, російська влада використовує пропагадну за допомогою одного з найпоширеніших джерел інформації – телебачення. Відповідно впроваджуючи ідеї, які вигідні для Кремля, що являє наслідком здійснення деструктивного впливу на свідомість та підсвідомість осіб, на яких спрямовано проведення СІО.

Література

1. Горбулін В. "Гібридна війна" як ключовий інструмент російської геостратегії реваншу. – Дзеркало тижня, 2015р., № 2, http://gazeta.dt.ua/internal/ gibridna-viyna-yak-klyuchoviy-instrumentrosiyskoyi-geostrategiyi-revanshu-.html.

УДК 355/359

Загребельний В.С.
Хмельницький О.О.
кандидат педагогічних наук,
Національна академія Служби безпеки України

НОВІТНІ МЕТОДИ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

На сьогоднішній день в світі протікає безліч процесів, одним з найважливіших є інформація, яка створюється, змінюється, поширюється. Небезпідставно існує вислів «Хто володіє інформацією – той володіє світом»,

значення цього вислову можна тлумачити, як те, що інформація має величезну силу впливу. За допомогою спеціальних інформаційних операцій (СІО) і здійснюється вплив, саме тому важливо досліджувати зазначене питання, щоб розуміти протікання процесу та мати змогу керувати ним.

Практичне значення отриманих результатів полягає у глибокому вивченні та розумінні сутності СІО та способи їх втілення.

В теперішній час ми спостерігаємо інформаційні процеси, які протікали раніше та не припиняються ні на секунду, адже інформація створюється та розповсюджується завжди. Шляхи використання та вплив інформаційних операцій потребує глибокого вивчення, адже шляхи використання та вплив інформаційних операцій потребує глибокого вивчення.

З давніх часів інформація відігравала важливу роль у житті людства, адже при володінні певної інформації можливо перемагати у війнах, отримувати перевагу над опонентом. Саме тому інформація стала найбільшою цінністю.

У роки будь якої війни, знавши певну інформацію про ворога, наприклад розташування його військ, їх чисельність та озброєння, давало можливість прийняти рішення щодо дій, які в кінцевому результаті приводили до перемоги над ворогом.

Перш за все потрібно зазначити визначення спеціальній інформаційній операції, **СІО** – це комплекс заходів інформаційного, психологічного, технічного впливу на об’єкт проведення операції, метою якого є деструктивний вплив на морально – психологічний стан об’єкта, зруйнування системи державного управління, переорієнтування на нав’язані цілі, цінності та ідеали.

Основними методами проведення СІО вважається:

Дезінформування, пропаганда, диверсифікація громадської думки, психологічний тиск, поширення чуток.

Розглянемо кожний метод окремо та більш детально:

1. Дезінформація – один з методів проведення спеціальної інформаційної операції, який здійснюється за допомогою надання неправдивої інформації, обману, створення умов для здійснення попередньо запрограмованих дій об’єктом СІО.

2. Пропаганда – створення та розповсюдження різних політичних, філософських, художніх, наукових ідей, збільшення частоти їх оприлюднення та доведення до відома об’єкту СІО, тим самим упровадження зазначених ідей в громадську думку, тобто здійснення впливу на свідомість та підсвідомість об’єкту.

3. Диверсифікація громадської думки – створення та надання хибної важливості дрібним питанням, акцентуванням на них особливої уваги, тим самим відволікання від реальних проблем, які потребують термінового, невідкладного вирішення.

4. Психологічний тиск – здійснення впливу на свідомість та підсвідомість об'єкту спеціальної інформаційної операції шляхом погроз, деструктивного впливу на особу та її свідомість, здійснення залякування, нав'язування запланованої моделі поведінки.

5. Поширення чуток – метод, при якому здійснюється поширення неправдивої інформації, зазвичай неофіційними джерелами інформації, серед широких верств населення з метою дезорганізації об'єкта СІО.

Основними цілями СІО визначено:

1. За мирного часу: домінування в інформаційному просторі, вплив на соціально – політичну ситуацію в регіоні, консолідація дружніх та нейтральних сил, формування власного позитивного іміджу.

2. У воєнний час: інформаційно – психологічне забезпечення вищого воєнно – політичного керівництва, поглиблення розбіжностей між армією і народом, підрив морально – бойового духу військ, переконання противника у необхідності відмови від агресії.

3. У післявоєнний час: забезпечення процесу формування лояльної влади, сприяння соціально – економічному розвитку в регіоні, протидія опозиційним проявам, впровадження програми гуманітарної допомоги.

Основні завдання СІО:

1. Послаблення міжнародних позицій країн, підрив їх національно – державного устрою.

2. Порушення системи державного управління за рахунок інформаційно – психологічного впливу на політичну, економічну, воєнну, соціальну і духовну сфери НБ.

3. Досягнення та утримання інформаційно – психологічної переваги над противником за рахунок здійснення комплексу соціальних заходів.

Висновки. Отже, ми проаналізували та дослідили визначення терміну СІО, розглянули основні методи проведення, такі як: дезінформування, пропаганда, диверсифікація громадської думки, психологічний тиск та поширення чуток.

УДК : 351.86:659.3/.4:004.738.5

Заскока Ю.В.
Національна академія державного управління
при Президентові України

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Сучасна система кібербезпеки України знаходиться на шляху розбудови. Критична інфраструктура країни стає об'єктом постійних кібератак,

завдяки чому Україну називають кіберполігоном для ворожих хакерів. Але атаки на критичну інфраструктуру зі зловмисними намірами це проблема глобальна, від ней потрапляють більшість сучасних країн світу. Інтернет має децентралізовану архітектуру та може зберігати експоненціальне збільшення обсягів трафіку, залишаючись постійною мішенню для зловмисних атак. Водночас, продовжує зростати залежність від основних функцій глобальної та відкритої мережі Інтернет, таких як система доменних імен (DNS), та основних Інтернет-служб для зв'язку та хостингу, програм та даних. Такі послуги дедалі більше зосереджуються в руках декількох приватних глобальних компаній. Це залишає національну економіку та суспільство вразливими до руйнівних геополітичних чи технічних подій. Збільшення використання Інтернету та зміна старих схем, спричинені пандемією, викрили ще більшу вразливість ланцюгів поставок, які залежать від цієї цифрової інфраструктури.

Прийнята у грудні 2020 року Стратегія кібербезпеки ЄС наголошує на трьох основних управлінських інструментах боротьби з кіберзагрозами: регуляторного, інвестиційного та політичного для застосування у трьох сферах діяльності ЄС – 1) стійкість; технологічний суверенітет та лідерство, 2) нарощування оперативного потенціалу для запобігання, стримування та реагування та 3) забезпечення глобального та відкритого кіберпростору[2].

Згідно оперативній інформації Держспецзв'язку щодо захисту державних інформаційних ресурсів за перший тиждень 2021 року Система захищеного доступу державних органів до мережі Інтернет заблокувала 76 328 атак різних видів, що на 32% більше, ніж попереднього тижня. Переважна більшість - це мережеві атаки прикладного рівня (99%). Також зафіксовано і заблоковано 16 DDoS-атак, зокрема на вебресурси НАБУ та Держспецзв'язку[1]. В цілому, протягом 2020 року було зафіксовано безліч випадків загроз кібербезпеці, пов'язаних із такими важливими інфраструктурами як фінанси та енергетика. Особливо сильно постраждали організації та спеціалісти у сфері охорони здоров'я під час пандемії. Оскільки технології стають невід'ємною частиною фізичного світу, кібератаки ставлять під загрозу життя та благополуччя найбільш вразливої частини населення.

Основні проблеми, щодо забезпечення кібернетичної безпеки об'єктів критичної інфраструктури України можна узагальнити такими блоками:

- неефективне (застаріле) нормативно-правове забезпечення процесу кібербезпеки країни;
- нефективна система реагування на кіберінциденти (технологічне відставання, нестача кваліфікованих кадрів, децентралізація управління);
- слабка взаємодія державних та недержавних суб'єктів у процесі забезпечення кібербезпеки держави;
- слабка система кіберрозвідки (Threat Intelligence);
- застаріла система стандартизації у сфері кібербезпеки

Критична інфраструктура та базові інформаційні послуги, що надає держава стають дедалі більше взаємозалежними та цифровими. Усі підключені до Інтернету пристрої будь то автоматизовані машини, системи промислового управління чи побутова техніка, та цілі ланцюжки поставок, які роблять їх доступними, повинні бути захищеними, стійкими до кібератак і мати здатність швидко відновлюватися у випадку виявлення вразливих місць. Це є фундаментальним для надання приватному та державному сектору України можливості вибору з найбільш безпечних інфраструктур та послуг. Наступне десятиліття во всьому світі — це можливість очолити розвиток безпечних технологій у всьому ланцюжку поставок. Забезпечення стійкості та посилення промислового та технологічного потенціалу в галузі кібербезпеки має мобілізувати всі необхідні законодавчі, інвестиційні та політичні інструменти. Кібербезпека промислових процесів, операцій та пристроїв може зменшити ризики, потенційно знизити витрати як для компаній, так і для суспільства в цілому, а отже, підвищити кіберстійкість держави.

Література

1. Оперативна інформація Держспецзв'язку щодо захисту державних інформаційних ресурсів за період з 30 грудня 2020 по 05 січня 2021 року. URL: https://cip.gov.ua/ua/news/operativna-informaciya-derzhspeczv-yazku-shodo-zakhistu-derzhavnikh-informaciinikh-resursiv-za-period-z-30-grudnya-2020-po-05-sichnya-2021-roku.
2. Стратегія кібербезпеки ЄС. URL: http://bit.ly/3ag55OJ.

УДК:681.3.06

Ільїн Д.В.
Фараон С.І.
Національний університет оборони України
імені Івана Черняховського

ВИКОРИСТАННЯ ПРИСТРОЇВ АУТЕНТИФІКАЦІЇ ДЛЯ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Виклики та загрози з якими зіштовхуються органи державної влади, місцевого самоврядування України та збройні формування України в сучасних реаліях протистояння агресії Російської Федерації, вимагають сучасних та ефективних рішень, щодо вирішення проблемних питань забезпечення кібербезпеки інформаційно-телекомунікаційних систем (згідно Закону України "Про основні засади забезпечення кібербезпеки України" від-

носяться до об’єктів інформаційної критичної інформаційної інфраструктури), що використовуються для автоматизації процесів управління та забезпечення процесів повсякденної життєдіяльності.

Складовими інформаційно-телекомунікаційної системи є лінії зв’язку, комутатори, маршрутизатори, сервери та персональні електронно-обчислювальні машини. І якщо для активного мережевого обладнання, серверів та персональних електронно-обчислювальних машин може бути створена комплексна система захисту інформації та забезпечені належні умови захисту від ведення технічної розвідки, то лінії звя’ку, переважно, простягаються поза межами зони в якій може бути забезпечений такий захист. Наслідком можуть стати: несанкціоноване підключення до ліній зв’язку та перехоплення трафіку, як на обладнанні провайдера так і вздовж всієї довжини ліній зв’язку, та проведення комп’ютерних атак з подальшим несанкціонованим доступом до серверів та персональних електронно-обчислювальних машин.

В умовах поширення пандемії коронавірусу з’явилась необхідність в дистанційній роботі працівників, що створює додаткові загрози для інформаційно-телекомунікаційних систем. Забезпечити безпеку використання віддалених робочих місць набагато складніше порівняно з локальними користувачами організації.

Віддалене робоче місце користувача породжує, в порівнянні з локальним офісним робочим місцем, три додаткових чинника загроз:

1. віддалений користувач знаходиться поза зоною фізичного контролю організації, необхідний доказ того, що до корпоративного ресурсу підключається саме співробітник компанії, а не зловмисник;

2. дані віддаленого користувача поширюються по каналах, які знаходяться поза зоною контролю організації;

3. для віддаленого робочого місця компанія не може забезпечити фізичну безпеку.

При організації віддаленого доступу повинні забезпечуватися три основні принципи інформаційної безпеки:

4. конфіденційність (інформація повинна бути доступна тільки особам, яким надано право користуватись даною інформацією);

5. цілісність (зміни інформації, що призводять до її втрати чи руйнуванню, повинні бути виключені);

6. доступність (інформація повинна бути доступна авторизованим користувачам, коли вона їм необхідна).

Для організації захисту ліній зв’язку та роботи віддалених робочих місць необхідно використовувати наступні механізми захисту:

7. надійні засоби аутентифікації користувачів;

8. систему розмежування доступу до інформаційних ресурсів на основі аутентифікаційних даних;

9. засоби організації VPN (апаратні пристрої та програмні рішення).

VPN з'єднання забезпечує підключення віддаленого користувача до ресурсів організації, об'єднання філіалів організацій, доступ віддалених користувачів до мережі інтернет через захищений сервер доступу організації, захист від перехоплення трафіку сторонніми особами на лініях зв'язку та обладнанні провайдерів.

Безпека VPN з'єднання досягається необхідною та достатньою довжиною ключа шифрування, частотою заміни ключа шифрування, забезпеченням безпечної аутентифікації користувача та системи сертифікації.

Використання логіну та паролю в класичному розумінні для аутентифікації у VPN не є безпечним варіантом. Користувач може забути свої аутентифікаційні дані, використовувати нестійкі паролі, пароль може бути отриманий від користувача внаслідок впливу на нього, інша людина яка дізналася пароль може скористатися їм без відома користувача.

Рішенням є використання пристрою аутентифікації, що забезпечує двофакторну перевірку для забезпечення доступу користувача. Ключ на пристрої є стійким, унікальним, його не можна скопіювати з пристрою та відтворити. Також апаратний носій забезпечує регламентовану зміну аутентифікаційних даних користувача. При компрометації пристрою його дія може бути припинена на сервері організації.

Таким чином використання в комплексі шифрування каналу зв'язку засобами VPN та двофакторної аутентифікації за допомогою пристрою аутентифікації забезпечить підвищення рівня кібербезпеки інформаційно-телекомунікаційних систем органів державної влади, місцевого самоврядування, збройних формувань України, підвищить рівень ефективності їх використання для забезпечення автоматизації процесів управління та повсякденної життєдіяльності.

УДК 355.451

Ільїн Р.О.
Розвадовський О.Б.
доктор юридичних наук,
Національна академія Служби безпеки України

ВПЛИВ КОРОНАВІРУСУ НА КІБЕРБЕЗПЕКУ

Пандемія коронавірусу (COVID-19) надзвичайно зростає і порушує глобальне здоров'я в основному, крім збитків для економіки, соціальних та політичних систем. Що ще важливіше, цифровий світ також знаходиться на межі руйнування, оскільки через цю загрозу люди у великих масштабах

змушені працювати віддалено, і це змусить їх сильно покладатися на віддалений зв'язок та цифрові інструменти. Кібер-зловмисники використовують цю ситуацію, намагаючись поставити під загрозу конфіденційність, цілісність та доступність даних [1].

Cynet виявив, що вірус Corona має значний вплив на інформаційну безпеку, і суб'єкти загроз активно використовують ці кризи. В даний час кіберзловмисники використовують дві основні тенденції: шкідливі атаки на електронну пошту та атаки на облікові дані віддалених користувачів. Всім компаніям доручають вести свою діяльність віддалено, якщо вірус корони повністю не врегульовано. Тепер співробітники значною мірою покладаються на спілкування електронною поштою. Cynet виявив, що 21% електронних листів включали шкідливі вкладення з більш розширеними можливостями, такими як перенаправлення на шкідливі веб-сайти або шкідливі макроси та експлойти. Сьогодні через пандемію вірусу корона (COVID-19) соціальна взаємодія та розповсюдження інформації швидко обмежуються такими цифровими засобами, як голосові дзвінки, відеодзвінки та текстові повідомлення. Наприклад, уряд Великобританії зробив цифровий "режим зв'язку за замовчуванням". Вони закликають громадян користуватися офіційними веб-сайтами уряду для оновлення. Тим часом вони також наголошують на невикористанні телефонних послуг, особливо тих, що просять отримати конфіденційну інформацію чи інші запити [2].

Нещодавно кіберзлочинці напали на Міністерство охорони здоров'я та соціальних служб США та веб-сайт статистики вірусу корона: worldometers.info з підлою метою порушити інформаційний потік та діяльність. Невизначеність і страх - це найбільші слабкі сторони людей. У цій конкретній долі пандемії Корони люди частіше припускаються помилок, ніж раніше. Стрес може заманити вас на дії, такі як натискання на шкідливі посилання, що включають так звані профілактичні заходи проти вірусу Corona, і ці дії можуть нашкодити конфіденційності критично важливих даних та інформації. Нещодавно новини про хаки повідомили про атаку, в результаті якої на карті було відображено шкідливе програмне забезпечення, яке відображало статистику вірусу Corona (COVID-19). Карта зберігалася у зловмисному додатку, і її завантаження завдало величезної шкоди конфіденційній інформації, такій як банківські реквізити, військові таємниці або номери соціального страхування. Хоча криза вірусу корона є серйозною, вам слід уникати різного роду посилань про вірус чи статистику захворюваності, щоб не стати жертвою кібератак [3]. Нижче наведено список деяких профілактичних заходів щодо коронавірусу та кібербезпеки:

- Не покладайтесь на неофіційні веб-сайти. Довіряйте лише офіційним веб-сайтам департаменту охорони здоров'я вашої країни.
- Будьте в курсі останніх оновлень Всесвітньої організації охорони здоров'я (ВООЗ). Не станьте жертвою шахрайського веб-сайту ВООЗ.

Щодо рекомендацій громадськості щодо хвороби коронавірусу ВООЗ (COVID-19), відвідайте офіційний веб-сайт ВООЗ: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public

- Не довіряйте телефонним дзвінкам з проханням надати конфіденційну інформацію.
- Уникайте відвідування фішингових електронних листів, включаючи карти чи інші вкладення щодо коронавірусу.
- Використовуйте фільтри спаму електронної пошти інших відомих програм захисту інформації, таких як Оркестрація безпеки, Автоматизація та відповідь (SOAR) та Інформація про безпеку та управління подіями (SIEM).

Література

1. Кібербезпека - KPMG Ukraine - KPMG International.
2. Coronavirus and Cyber Security - assets.kpmg.
3. Бізнес в умовах COVID-19: конфіденційність та ... - Everlegal
everlegal.ua › biznes-v-umovakh-covid-19-konfidentsi.

УДК 355.01

Ісайко Д.І.
Національна академія Служби безпеки України

ІНФОРМАЦІЙНА ВІЙНА

Сьогодні існує ворожнеча між різними країнами, однак, проведення війни в розумінні військових дій, як це відбувалось раніше – не є доцільним, адже це потребує більшої кількості витрат на зброю, людей, та ефективність не завжди є такою, яку вираховували при підготовці до військових дій. Саме через ці причини військові дії перенеслись у інформаційний простір, адже розвиток науки та техніки дозволяє це застосовувати.

Під інформаційною війною будемо розуміти проведення широкомасштабних інформаційних дій, що застосовуються сторонами, які знаходяться у протиборстві, направлених проти соціальних та інформаційно-технічних систем держави з метою одержання інформаційної переваги над противником [1].

Розглянемо завдання, виконання яких досягається за допомогою проведення інформаційної війни.

Завдання інформаційної війни:

– створення атмосфери бездуховності, негативного ставлення до культури та історичної спадщини у суспільстві конкурента чи ворога;

– маніпулювання громадською думкою і політичною орієнтацією населення держави з метою створення політичного напруження та стану, близького до хаосу;

– дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою розпалення конфліктів, стимулювання недовіри, підозри, загострення ворожнечі, боротьба за владу;

Велике значення має визначення об'єктів інформаційної війни.

Загалом об'єкт – це те, на що спрямовано певну діяльність, тобто те, на що суб'єкт інформаційної війни намагається вплинути з метою досягнення позитивного для нього результату.

Отже, головний об'єкт, на якому концентрується безпосередній інформаційний деструктивний вплив у межах заходів інформаційної війни, – громадська думка та свідомість окремої людини.

Основними об'єктами деструктивного інформаційного впливу є:

– ідеологічно-психологічне середовище суспільства, пов'язане з використанням інформації, інформаційних ресурсів та інформаційної інфраструктури для здійснення впливу на психіку і поведінку людей;

– ресурси, які розкривають духовні, культурні, історичні, національні цінності, традиції, надбання держави, нації в різник сферах життя суспільства;

– інформаційна інфраструктура, тобто абсолютно всі проміжні ланки між інформацією та людиною;

– система формування суспільної свідомості (світогляд, політичні погляди, загальноприйняті правила поведінки тощо);

– система формування громадської думки;

– система розроблення та прийняття політичних рішень;

– свідомість та поведінка людини [2].

Існують різновиди інформаційних війн, які відрізняються за своєю специфікою та сферами впливу.

Види інформаційних війн:

– психологічна війна;

– кібервійна;

– мережева війна;

– ідеологічна війна;

Метою інформаційної війни є порушення обміну інформацією в таборі конкурента. Неважко зрозуміти, що цей вид зброї, як правило, взагалі не спрямований на завдання втрат у живій силі. У цьому сенсі крива технології вивела, нарешті, до безкровної і, водночас, винятково ефективної зброї. Вона знищує не населення, а державний механізм [3].

Висновки. Отже, можемо зробити висновок, що ми дослідили сутність інформаційної війни, дали визначення, а саме: під інформаційною війною будемо розуміти проведення широкомасштабних інформаційних дій, що застосовуються сторонами, які знаходяться у протиборстві, направлених

проти соціальних та інформаційно-технічних систем держави з метою одержання інформаційної переваги над противником, також зазначили задання ІВ, дослідили об'єкти інформаційних війн, а також види інформаційної війни.

Література

1. Енциклопедія сучасної України. [Електронний ресурс] — Режим доступу: http://esu.com.ua/search_articles.php?id=12460.

2. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / Валентин Петрик. — Режим доступу : www.justinian.com.ua/article.php.

3. Шаравов И.К вопросу об информационной войне и информационном оружии // Зарубежное военное обозрение – 2002. – Вип. №10. – С. 3-5.

УДК 351.86:316.658

Канарський В.С.
Національна академія державного управління
при Президентові України

ПРІОРИТЕТИ ДЕРЖАВНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Політика національної безпеки повинна бути спрямована передусім на захист національних цінностей і реалізацію національних інтересів. Ключовим завданням є не стільки реагування на загрози, як їх попередження. Важливою є готовність до реалізації національних інтересів в умовах швидких змін геополітичної та внутрішньополітичної ситуації. Органи державного управління повинні попереджати й нейтралізувати явища і процеси, що перешкоджають реалізації внутрішніх і зовнішніх національних інтересів, а не просто захищати їх від загроз[2].

Важливою складовою загальної політики забезпечення інформаційної безпеки України є підвищення участі громадськості у процесах удосконалення зв'язку "суспільство – держава". Подальше зміцнення інформаційної безпеки країни вбачається у спільних, злагоджених діях усіх державних інституцій, громадськості, медіа-спільноти[3].

Серед пріоритетів державної політики у сфері інформаційної безпеки можна виділити такі основні напрями:

Захист життєво важливих інформаційних інтересів особистості, суспільства та держави від внутрішніх і зовнішніх загроз. Враховуючи сучасні загрози національній безпеці України, цей напрям повинен конце-

нтруватись на протидії викликам, що пов'язані із застосуванням інформаційних технологій у військово-політичних цілях, у тому числі для здійснення ворожих дій і актів агресії, спрямованих на підрив суверенітету, порушення територіальної цілісності держави. У цьому контексті першочерговими заходами мають стати:

- удосконалення існуючої системи забезпечення ІБ ЗСУ, військових формувань і органів, що включає в себе сили і засоби інформаційного протиборства;
- розробка та впровадження дієвих механізмів прогнозування, виявлення та оцінки інформаційних загроз;
- нейтралізація інформаційно-психологічного впливу населення країни, в тому числі спрямованого на підрив національних цінностей та історичної спадщини [1];
- наповнення національного інформаційного простору високоякісним і конкурентоздатним вітчизняним інформаційним контентом, що є необхідним засобом впливу на формування громадської й індивідуальної свідомості, становлення громадянського суспільства;
- поширення якісного національного інформаційного продукту на тимчасово окупованих територіях, розробка та впровадження цілісної державної інформаційної політки щодо тимчасово окупованих територій;
- надання постійної психологічної підтримки населенню на окупованих та прифронтових територіях, а також у населених пунктах поблизу зони розмежування;
- розвиток системи медіаграмотності населення країни, інформаційної культури, профілактика правопорушень в інформаційній сфері;
- правове врегулювання відносин у сфері державної політики ІБ та визначення правових механізмів взаємодії і співпраці державних інститутів з політичними партіями та громадськими організаціями. На рівні законів доцільно визначити систему правового регулювання стосовно: недержавного забезпечення національної безпеки та її інформаційної складової; засад громадського контролю за діяльністю органів державної влади і місцевого самоврядування [60, с.69].

Захист критичної інформаційної інфраструктури. Серед заходів цього напряму доречно передбачити:

- підвищення захищеності критичної інформаційної інфраструктури та стійкості її функціонування;
- розвиток механізмів виявлення та попередження інформаційних загроз і ліквідації наслідків їх прояву, викликаних інформаційно-технічним впливом на об'єкти критичної інформаційної інфраструктури;
- створення єдиної системи стандартів з інформаційних технологій, сертифікації засобів інформатизації; підвищення інвестиційної привабливості у сфері інформатизації тощо;

• напрацювання системи ефективних взаємовідносин між державою та приватним сектором, без участі якого кібербезпека держави є просто неможливою, адже багато кіберактивістів (хактивистів) активно протидіють намаганням агресора використати кіберпростір проти інтересів України;

• розробка механізмів обміну інформацією з країнами ЄС та НАТО щодо передових практик в сфері забезпечення безпеки функціонування елементів критичної інфраструктури.

Література

1. Дмитренко М. А. Проблемні питання інформаційної безпеки України. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3318/2997.

2. Садовський В; Дацюк А; Марутян Р, Ніцой О. Як визначати пріоритети державної безпекової політики. URL: http://euinfocenter.rada.gov.ua/uploads/documents/28991.pdf.

3. Солодка О.М., Пріоритети удосконалення інформаційної безпеки України. Інформація і право. № 3(15). 2015 URL: http://ippi.org.ua/sites/default/files/solodka.pdf.

4. Сніцаренко П. М. Удосконалення чинного інформаційного законодавства України як необхідна умова адекватності заходів щодо забезпечення інформаційної безпеки держави. Зб. наук. пр. Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2018. № 2(63). С. 68-74.

УДК 355

Кириченко Є. О.
Національна академія Служби безпеки України

ФОРМИ І ЗАСОБИ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ БОРОТЬБИ

На сьогоднішній день триває інформаційна боротьба між багатьма країнами, це постійний процес, який ніколи не припиняється, адже з давніх часів здійснювалось інформаційне протиборство. Яскравим прикладом є холодна війна, в якій і відбувалось інформаційне протистояння США та СРСР. Дослідження інформаційної боротьби сьогодні – важлива складова в боротьбі та зайнятті лідерських позицій на світовому просторі.

Кожного дня відбуваються різні інформаційні процеси, під час яких створюється інформація, змінюється та зазнає перетворень. Інформація є найважливішим ресурсом, саме тому існують різні способи її використання. Одним з таких способів є інформаційне протиборство, це означає, що зброя – це інформація.

Інформаційна боротьба - це сукупність узгоджених та взаємопов'язаних за метою, завданнями, об'єктами впливу і часом інформаційних операцій, ударів, акцій і атак, котрі проводяться як послідовно, так і одночасно в кількох сферах життєдіяльності держави з метою сприяння досягненню визначених цілей власної національної політики [1].

Інформаційна зброя - це сукупність засобів і технологій, призначених для ведення інформаційної боротьби. За об'єктами впливу інформаційну зброю можна поділити на два основних класи:

1. Інформаційно-технічна зброя, що впливає на інформаційні ресурси, інформаційну інфраструктуру збройних сил, держави в цілому.

2. Інформаційно-психологічна зброя, що впливає на морально-психологічний стан людини, соціальних та інших груп населення, суспільства в цілому.

Існуть форми ведення інформаційної боротьби, однією з найважливіших та популярних форм є інформаційно – психологічна операція.

Інформаційно-психологічні операції (далі - ІПсО) розглядаються як форма ведення психологічної боротьби та передбачають використання складної сукупності різних видів, способів і прийомів інформаційно-психологічного впливу, тобто впливу інформацією. ІПсО починають проводиться в мирний час, активізуються в загрозливий період і повною мірою розгортаються у ході бойових дій.

Зміст ІПсО в загрозливий період конкретизується в залежності від політичних і військових цілей конфлікту, військово-політичної обстановки на ТВД; розмаху діяльності опозиційних політичних партій, дисидентського та пацифістського рухів, а також особливостей психології, звичаїв, традицій і релігійних вірувань народу в країні противника.

У ході бойових дій ІПсО переслідують наступні головні цілі:

- підрив морально-психологічного стану особового складу збройних сил противника;

- послаблення наступального пориву або здатності до завзятої оборони противника;

- деморалізація частин противника, що відходять, спонукання особового складу оточених (відсічених) підрозділів до здачі в полон.

Основними об'єктами ІПсО виступають:

1) військовослужбовці противника;

2) населення противника;

3) населення і військовослужбовці нейтральних і союзних держав.

4) військовослужбовці та населення своєї країни [2].

Висновки. Отже, ми провели дослідження інформаційної боротьби, а саме: провели дослідження інформаційної зброї, цілі інформаційно – психологічних операцій, визначили об'єкти інформаційно – психологічних операцій. Інформація стала найважливішим ресурсом, саме тому вона несе в собі велику силу, як створення чогось нового, так і руйнування.

Література

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

2. Расторгуев С. П. Информационная война / С. П. Расторгуев. – М. : Радио и связь, 1999. – 416 с.

УДК 321.011
Ковтун А.О.
Національна академія Служби безпеки України

ДЕФІНІЦІЯ «ІНФОРМАЦІЙНА БЕЗПЕКА» ТА ЇЇ МІСЦЕ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Сьогодні питання інформаційної безпеки займають одне з найперших місць в усіх сферах життєдіяльності людини, суспільства та держави. Доктринальних визначень дефініції інформаційної безпеки існує дуже багато, однак досі немає єдиної думки щодо її сутності.

За науковими напрацюваннями В. Гурковського, інформаційна безпека держави – «це суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворювальної нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів» [1, с. 74].

О. Баранов виокремлює категорію національних інтересів, визначаючи інформаційну безпеку як «стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації й несанкціоноване її поширення та використання, а також через негативний інформаційний вплив і негативні наслідки функціонування інформаційних технологій» [2, с. 60-62].

«Інформаційну безпеку як стан захищеності національних інтересів України в інформаційній сфері від загроз особі, суспільству, державі через неповноту, несвоєчасність інформації, несанкціоноване поширення та використання інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій» визначають О. Гладун і В. Шатун [3, с. 175].

В.Ліпкан, Л.Харченко та О.Логінов розглядають інформаційну безпеку як «процес управління загрозами та небезпеками державними й недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України» [4, с. 75].

Р. Калюжний вважає, що «інформаційна безпека – це вид суспільних інформаційних правовідносин стосовно створення, підтримки, охорони та захисту бажаних для людини, суспільства й держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов'язані зі створенням, зберіганням, поширенням і використанням інформації» [5, с. 18-19].

Б.Кормич вважає, що «інформаційна безпека - це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування й розвитку людини, всього суспільства та держави» [6].

І.Панарін визначає інформаційну безпеку як «стан інформаційного середовища суспільства і політичної еліти, що забезпечує його формування і розвиток в інтересах керівництва країни, громадян і суспільства» [7, с. 128].

Говорячи про нормативне визначення даного поняття, слід зазначити, що жоден нормативно-правовий акт не дає трактування «інформаційної безпеки». Проте, майже всі нормативно-правові акти у сфері інформаційної безпеки тим чи іншим способом торкаються її аспектів.

Зіставляючи визначення родового поняття «національна безпека України - захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз», що міститься в ст.1 ЗУ «Про національну безпеку», і визначення поняття «інформаційна безпека України», що відсутнє у нормативних актах України, проте розглянуте в рамках наукової розвідки відзначимо, що в обох випадках загальним є «стан захищеності», але на цьому схожість закінчується. Таким чином, у наявності маємо невизначеність і теоретичну неузгодженість наявних дефініцій ключових понять і пріоритетів у сфері безпеки.

Отже, виходячи із вищевикладеного, інформаційну безпеку необхідно розглядати не тільки як окремий фактор, а як необхідний структурний елемент національної безпеки в цілому по-перше, а по-друге, виникає нагальна потреба у визначенні національних інтересів (особи, суспільства, держави) в інформаційній сфері та фіксування конкретних дефініцій в національному законодавстві.

Література

1. Гурковський В.І. Безпека як об’єкт правовідносин в умовах глобального інформаційного суспільства. Правова інформатика. 2010. № 2(26). С. 72-77.

2. Баранов О.П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України. Вісник Національної академії державного управління при Президентові України. 2014. № 3. С. 60-65.

3. Шатун В. Т. Інформаційна безпека – невід’ємна складова національної безпеки України. Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія». 2016. Т. 267. Вип. 255. С. 174-180.

4. Ліпкан В. А., Харченко Л. С., Логінов О. В. Інформаційна безпека України: Глосарій. К.: Текст, 2004. 136 с.

5. Калюжний Р. Питання концепції реформування інформаційного законодавства України. Правове, нормативне та метрологічне забезпечення системи інформації в Україні: Тематичний збірник праць учасників Другої науково-технічної конференції. К., 2000. С.17-21.

6. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: [навчальний посібник]. Київ: Кондор, 2004. 382 с.

7. Панарин И. Технология информационной войны: [монографія]. М.: КСП+, 2003. 320 с.

УДК 316.422

Котляров Д.П.
Семеній Д.М.
Національна академія Служби безпеки України

НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Кібербезпека є однією із складових частин національної безпеки України. Вона пов'язана із стратегією формування виваженої державної політики, забезпечення інформаційної безпеки, яка повинна передбачати систему заходів державного та міжнародного характеру, належне місце в якому займає кібербезпека.

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 [1].

Кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет [1].

Сучасний кіберпростір обумовлений виникнення нових загроз національній і міжнародній безпеці. Поряд з інцидентами природного походження зростає кількість і потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Аналіз існуючих тенденцій свідчить, що окремі держави для реалізації власної протиправної мети починають дедалі частіше вдаватися до кібератак. Сьогодні комп'ютерні атаки, як правило, направлені за трьома ключовими напрями:

– виведення з ладу інформаційно-телекомунікаційної системи (ІТКС) та критичної інфраструктури за допомогою вірусів та спаму;

– несанкціонований доступ у систему з метою викрадення даних;

– незаконне оприлюднення персональних даних у мережі Інтернет.

В нашій країні 27 червня 2016 року потужний комп'ютерний вірус "Petya A" паралізував роботу низки компаній в Україні. Найбільш уразливими виявились українські компанії та відомства. Серед постраждалих - уряд України, національна пошта, міжнародний аеропорт "Бориспіль", Чорнобильська АЕС, а також низка ЗМІ, банків, комерційних структур.

Виникає необхідність нейтралізації подібних загроз, тому без основоположного закону навряд чи можливі інші рішення. На наш погляд, закон – теоретична, фундаментальна база, підзаконні акти деталізують шлях його імплементації. Наразі питання кібербезпеки регулюються базовим Законом України «Про основні засади забезпечення кібербезпеки України», Стратегією кібербезпеки України, Конвенцією про кіберзлочинність, Кримінальним кодексом України та іншими нормативно- правовими актами. Базовим законом встановлюється значна кількість понять, що є новими для правового поля України, зокрема «кібербезпека», «кіберзагроза», «кіберпростір», «кіберінцидент». Одним з об'єктів кібербезпеки та кіберзахисту Закон визначає об'єкти критичної інфраструктури.

Хоча законом і встановлено, що за порушення у сфері кібербезпеки особи несуть відповідальність згідно з цивільним, адміністративним та кримінальним законодавством, в кодексах відсутні будь-які згадки поняття "кіберпростір".

Основними проблемами, які потребують розв'язання, є:

- недостатність та неузгодженість нормативно-правового регулювання з питань кібербезпеки;
- відсутність державного органу, відповідального за координацію дій у сфері захисту критичної інфраструктури;
- відсутність єдиної методології проведення оцінки загроз в кіберпросторі;
- нерозвиненість державно-приватного партнерства у сфері захисту кібербезпеки.

Проблеми забезпечення захисту кібербезпеки передбачається розв'язати шляхом:

- створення механізму реалізації нормативно-правової бази з питань кібербезпеки та кіберзахисту;
- визначення повноважень, завдань та відповідальності суб'єктів державної системи захисту критичної інфраструктури.
- розроблення і затвердження єдиної методології проведення оцінки кібербезпеки об'єктів;
- розроблення переліку об'єктів критичної інфраструктури;

У Стратегії кібербезпеки України зазначається, що метою є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Слід зазначити, що у зв'язку з її реалізацією Рада національної безпеки і оборони України ухвалила рішення про створення спеціального органу як робочого органу – Національного координаційного центру кібербезпеки (НКЦБ) Центр повинен виявляти на ранніх стадіях виникнення кіберзагрози і забезпечувати швидку її локалізацію. Також НКЦБ надає рекомендації з питань кібератак, кіберзахисту та кібербезпеки для державних та приватних підприємств, з якими можна ознайомитися на сайті координаційного центру кібербезпеки

Отже, подальше вдосконалення нормативно-правових актів, процесів і технологій забезпечення кібербезпеки збільшить ефективність захисту кіберпростору України. Підвищення обізнаності, просвіта та навчання у відповідності до чітко визначених пріоритетів кібербезпеки, принципів, політики, процесів, програм є надзвичайно важливим компонентом забезпечення достатнього рівню кібербезпеки, і їм повинно приділяти уваги на усіх рівнях – політичному, законодавчому, економічному та регуляторному.

Література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VI. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2163-19.

УДК 327.5

Кудик П.О.
Національна академія Служби безпеки України

РОЛЬ ПРОПАГАНДИ І КОНТРПРОПАГАНДИ ПІД ЧАС ВЕДЕННЯ ГІБРИДНОЇ ВІЙНИ

Сьогоднішні військові дії на сході України, а також політичні, пропагандистські, економічні та інші аспекти, пов'язані з ними, експерти та вчені відносять до категорії «гідридні війни».

При проведенні гібридної війни Російської Федерації проти України особливе місце посідають акти інформаційного та психологічного впливу, що дозволяють країні-агресору досягти своїх цілей з порушенням міжнародного права, використовуючи людські ресурси країни - об'єкт втручання або агресії (в даному випадку Україна), а також людські ресурси. інших країн, одночасно зменшуючи вплив міжнародного співтовариства на власні агресивні дії.

Інформаційні технології в гібридному протистоянні є величезним фактором, оскільки можливість швидкого та необмеженого розповсюдження інформації через Інтернет, а також залучення професіоналів до створення

та відтворення контенту, стає найважливішим інструментом для громадської думки. Зрештою, відомо, що в кризових комунікаціях надзвичайна важливість інформаційної переваги - тобто чим раніше певне повідомлення доходить до аудиторії, тим краще. Таким чином, ведення пропагандистських операцій значно спрощується, тоді як реагування агентів контрпропаганди та розповсюдження спростування значно ускладнюються механізмами тиражування вмісту (відтворення подібних повідомлень на великій кількості веб-сторінок). Крім того, першість публікації та її кількісна складова важливіші в механізмах оптимізації пошукових систем, які сьогодні «вибирають» для користувача Інтернету, яку інформацію він повинен прочитати першим і класифікувати її. Механізми оптимізації пошукових систем періодично змінюються, але адаптація засобів пропаганди під ці механізми також трансформується відповідно до вимог пошукових систем [1].

Суть контрпропаганди полягає у запобіганні та викритті фальшивої пропаганди політичних опонентів. Контрпропаганда виконує дві функції - попередження та викриття. Провідною є профілактична функція, метою якої є формування у свідомості людей чітких ідеологічних позицій, стійкого імунітету до ідеологічних чи ідеологічних впливів політичних опонентів, їх психологічного впливу. Його завдання полягає у формуванні поряд з іншими ідейно-політичної матриці сприйняття інформації, своєрідного ідеологічного імунітету. Викривальна функція полягає у розвінченні ідей, пропагандистських стереотипів, а також у поясненні суспільством навмисної дезінформації політичними опонентами. Контрпропаганда допомагає виявити руйнівний характер пропагандистських дій опонентів, їх спрямованість, розуміння методів і прийомів ворожої пропаганди. Це дозволяє протиставити дані пропаганди опонентів реальним фактам суспільно-політичного життя. Метод контрпропаганди полягає у здатності систематично демонструвати основу, мотиви та технологію обману і, зрештою, навчити людей самостійно викривати ідеологічні провокації політичних опонентів. Проблему контрпропаганди слід розглядати дещо в іншому ракурсі, а саме як ефективний наступ на пропаганду ворога шляхом знищення його іміджу шляхом публікації негативної інформації про аспекти його діяльності чи життя. Слід зазначити, що будь-яка успішна пропаганда політичного опонента завдає шкоди іншій партії, тому пошук слабких місць та їх використання в контрпропагандистській діяльності є виправданим. Можна погодитися з М. Кастельсом, що оскільки шанси політичного вибору залежать від сприйманих рис особистості, ефективна виборча кампанія завжди підкреслює позитивні якості кандидата, кидаючи глибоку тінь на його опонента. Більше того, негативні образи мають сильніший вплив на поведінку виборців, ніж позитивні [2, с. 268].

Руйнування політичного опонента через наклеп є найпотужнішою зброєю контрпропаганди. Це можна зробити різними способами: шляхом

вивчення репутації кандидата у приватному і в громадському житті; нав'язування виборцям прямо чи підсвідомо негативних стереотипів, пов'язаних з кандидатом; уточнення змісту заяв кандидата або політичних позицій з метою демонстрації їх суперечності з основними цінностями електорату; публікація порушень або суперечливих заяв осіб чи організацій, пов'язаних з кандидатом; розкриття фактів корупції, протиправної поведінки в партіях чи організаціях, які підтримують цю кандидатуру. У всіх випадках метою є викликати сумнів серед потенційних прихильників кандидата та мобілізувати конкуруючих виборців.

Таким чином, технології політичної контрпропаганди відіграють важливу роль у запобіганні та протидії пропаганді опонентів. Контрпропагандистські технології можна класифікувати відповідно до їх функціональної спрямованості. Технології контрпропаганди поділяються на превентивні, протидіючі (нейтралізуючі) та образливі. Технології попередження працюють, щоб передбачити реакцію опонента, пояснюючи ситуацію, перш ніж вона буде використана для негативних повідомлень опонента. Протидія технологіям пропаганди спрямована на зменшення або нейтралізацію пропаганди опонента. Контртехнології включають пряме спростування ворожої пропаганди, непряме спростування, відволікання уваги, мовчання (мовчання), обмежувальні заходи, імітація обману, попередження та мінімізація.

Література

1. Фісенко Т. В. Пропаганда як складник гібридної війни URL : http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/is_2017_25_7.pdf.

2. Кастельс М. Власть коммуникации : учеб. пособие / М. Кастельс ; пер. с англ. Н. М. Тылевич; под науч. ред. А. И. Черных ; Нац. исслед. ун-т «Высшая школа экономики». М. : Изд. дом Высшей школы экономики, 2016. С. 564.

УДК 329.09.5

Кульбачний М.С.
Національна академія Служби безпеки України

ІНФОРМАЦІЙНА БЕЗПЕКА: ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою для України.

Інформаційна безпека передбачає, перш за все, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Досягнення належного рівня національної безпеки сучасної держави неможливе без реалізації ефективної інформаційної політики [1].

Інформаційна безпека (Information Security) має три основні складові: конфіденційність, цілісність і доступність. Конфіденційність належить до захисту чутливої інформації від несанкціонованого доступу. Цілісність означає захист точності і повноти інформації і програмного забезпечення. Доступність – це забезпечення доступності інформації і основних послуг для користувача в потрібний для нього час.

Україна все частіше стикається з масштабними проявами інформаційної злочинності, що загрожують сталому та безпечному функціонуванню інформаційно-телекомунікаційних систем. Про високий рівень загроз у кібернетичному просторі України свідчать, наприклад, результати дослідження відомого німецького оператора зв'язку Deutsche Telecom, згідно яких наша країна опинилася на четвертій сходинці світового рейтингу серед країн – об'єктів і джерел кібернетичних атак. 37-й Президент США Річард Ніксон говорив: «Один долар, вкладений в інформацію і пропаганду, цінніший, ніж 10 доларів, вкладених у створення систем зброї, бо остання навряд чи буде вжита, в той час, як інформація працює щохвилинно і повсюдно [2].

З метою протидії масштабним негативним інформаційно-психологічним впливам пріоритетними напрямами національної інформаційної політики мають стати: 1) концептуальне переосмислення інформаційних завдань, що постали перед українською владою та суспільством загалом; 2) захист українського інформаційного простору від пропагандистської аудіовізуальної та друкованої продукції країни-агресора – Російської Федерації; 3) потужна фінансова, інформаційна та інституційна підтримка розвитку українського кінематографу, телевізійного контенту, радіо простору та книгодрукування; 4) побудова власної ефективної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства; 5) модернізація системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики; 6) удосконалення законодавства в сфері інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів; 7) розвиток національної інформаційної інфраструктури; 8) стимулювання підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг; 9) забезпечення потужної інформаційно-комунікативної присутності України в міжнародному інформаційному просторі [2].

Особливо складна сьогодні проблема завчасного створення засобів, необхідних для інформаційного протиборства, або, якщо користуватися американською термінологією, - «інформаційної війни».

Комісія з питань національної безпеки визначила такі потенційні загрози в інформаційній сфері: відсутність у міжнародного співтовариства об'єктивного уявлення про Україну; інформаційна експансія з боку інших країн; відтік інформації, що містить державну таємницю, а також конфіденціальної інформації, що є власністю держави; повільне входження України до світового інформаційного ринку; незбалансованість державної політики та відсутність необхідної інфраструктури в інформаційній сфері [2].

Враховуючи цілі та завдання політики інформаційної безпеки, виділимо чотири основні напрями забезпечення інформаційної безпеки: 1. Забезпечення інформаційної достатності для прийняття рішень. 2. Захист інформації, тобто захист інформаційного ресурсу. 3. Захист та контроль національного інформаційного простору, тобто систем формування масової свідомості. 4. Присутність у світовому інформаційному просторі [2].

Цікавим прикладом системи забезпечення збирання та аналітичної обробки інформації є діюча система США. В ній вирізняються такі три складові:

• державні інформаційні органи, зокрема розвідспільнота, установи держдепартаменту, адміністрації Президента, Ради національної безпеки;

• інформаційні центри «прямої підтримки», зокрема такі установи, як Rand, Військовий університет національної оборони тощо;

• громадські центри «широкої підтримки», такі, як Центр стратегічних і міжнародних досліджень, Американський підприємницький інститут, Фонд спадщини, Інститут Като, Атлантична Рада, Центр з національної політики та ін.

Поступово формується інформаційно-аналітичне середовище України. У 1992 р. розпочав свою діяльність Національний інститут стратегічних досліджень, який за статутом є «урядовою інституцією для проведення досліджень, аналітичного прогнозування та стратегічного планування з метою забезпечення інформацією Ради національної безпеки і оборони та Президента України». Але інформаційно-аналітичне середовище в Українській незалежній державі ще не повністю відповідає вимогам часу, потребує певної корекції щодо незалежності науково-аналітичних інституцій від політичних впливів, формування професійної, фахової спільноти тощо.[3]

Література

1. Боднар І.Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. №1. С. 68-75.

2. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Humanitarian vision. 2016. Vol. 2, № 1. С. 27-32.

3. Степанов В.Ю. Інформаційна безпека в інформаційній сфері державного управління. Теорія та практика державного управління. 2016. №4(55).

УДК 316.422
Ласкевич А.Р.
Вінницький Державний педагогічний університет
імені Коцюбинського

ОРГАНІЗАЦІЙНО-ПРАВОВІ ПРОБЛЕМИ ЗАХИСТУ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Шлях України у розбудові власної кібербезпеки потребує докорінних і невідкладних змін. Це не лише позиція лідерів вітчизняного кіберзахисту. Необхідність змін підтверджена атаками на об'єкти критичної інфраструктури, багатьма іншими інцидентами, які створили Україні сумнівну репутацію одного з головних кіберполігонів [1].

Законодавча база – важлива складова у забезпеченні інформаційної безпеки (ІБ) та кібербезпеки держави, однак, ураховуючи основні недоліки чинного законодавства у безпековій сфері, його пасивний характер, декларування теоретичних аспектів забезпечення ІБ, безпеки кіберпростору та протидії кіберзлочинності на рівні доктрин, указів, рішень тощо, потрібно розробити механізм практичного впровадження захисту інформації в кіберпросторі. Тобто задається «напрям», якого необхідно дотримуватися за відсутності правового, фінансового та кадрового забезпечення і без жодної відповідальності посадових осіб [2].

Безпека інформаційного і кіберпростору, запровадження диджиталізації процесів управління, гарантування безпеки й сталого функціонування національної критичної інфраструктури, інформаційних систем (ІС) повинні стати не тільки складовими державної політики у сфері розвитку кіберпростору та становлення інформаційного суспільства в Україні, а також включення цих чинників у сферу політичних пріоритетів держави [3].

На міжнародному і національному рівнях кіберзлочинність є однією з найгостріших проблем, яка постала сьогодні перед правоохоронними органами усіх держав. Досі не вироблений системний підхід у протидії кіберзлочинності з урахуванням сучасних викликів і загроз інформаційній безпеці [4].

У національній системі права першими та єдиними законодавчими актами у сфері протидії кіберзлочинності, як стратегічної позиції на найвищому політичному рівні, є Закон України «Про основні засади забезпечення кібербезпеки України» та Указ Президента України № 47/2017 про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Вони законодавчо закріпили кібербезпеку як пріоритет роботи для державних органів і уряду.

Ці докумети могли б стати основою для розробки ефективної, сучасної нормативно-правової бази, або для інших нормативно-правових актів, які б виконували ключову роль у забезпеченні кібербезпеки в Україні, але зрушень у цій сфері немає.

Тому, однією з основних проблем можна назвати неефективну нормативну правову базу та відсутність положень системи менеджменту у сфері нормативно-правового забезпечення інформаційних відносин, які могли б забезпечити динаміку процесів правового забезпечення інформаційної і кібербезпеки в Україні.

Ще однією з основних проблем є трансформація державного управління у сфері кібербезпеки. Є багато завдань в сфері кібербезпеки, які повинні формуватись і реалізовуватись на державному рівні , але державні структури не зможуть провести таку трансформацію. Тому, повинна бути створена організація, яка візьме на себе всі функції управління впровадженням програми з кібербезпеки та регулярного контролю за процесом упровадження. Тобто, це повинна бути неурядова структура, яка зможе впроваджувати реформи у сфері кібербезпеки [5].

Отже, наявна нормативно-правова база, яка, крім іншого, не охоплює всього спектра сучасних загроз кібернетичній безпеці держави, повинна бути істотно доповненою. На організаційно-правовому рівні необхідно чітко ідентифікувати проблему забезпечення кібербезпеки та своєчасно надавати нові, сучасні правові інструменти для протидії цим загрозам. 2. Пропонуємо внести зміни до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» і передбачити новий підхід до реалізації способу підтвердження відповідності інформаційної системи вимогам із захисту інформації шляхом установлення відповідних критеріїв. Мета такого заходу полягає у законодавчому закріпленні вимог стандартів сімейства систем менеджменту інформаційною безпекою для окремих категорій інформації, захист якої забезпечується законодавством України [5].

Література

1. Янковський О. Україні потрібна нова кіберстратегія.URL: https://www.pravda.com.ua/columns/ 2019/09/14/7226291/.

2. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби з кіберзлочинністю: основні напрями реформування. Аналітична записка. Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/articles/454/.

3. Рудий Т. В., Сеник В. В., Рудий А. Т., Сеник С. В. Організаційно-правові, криміналістичні та технічні аспекти протидії кіберзлочинності в Україні. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / гол. ред. Р. І. Благута. Львів : ЛьвДУВС, 2018. Вип. 1. С. 283–301.

4.Костенко О. В. Проблеми правового регулювання та розвиток кібернетичної безпеки України на сучасному етапі. Інформація і право. Науково-дослідний інститут інформатики і права Національної академії правових наук України. Київ, 2019. № 3 (30). С. 96–104.

5. http://www.sls.lvduvs.edu.ua/documents_pdf/arhiv/sps_3(9)_2020/04.pdf.

УДК 355.451
Липний С.І.
Шепета О. В.
кандидат юридичних наук, доцент,
Національна академія Служби безпеки України

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ЗАКОНОДАВСТВІ УКРАЇНИ: РЕАЛЬНІСТЬ І ПЕРСПЕКТИВИ

З кожним роком у світі безупинно зростає увага до питань інформаційної безпеки. Інформаційна сфера стала важливим чинником розвитку суспільства, активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки. Захист національних інтересів і національної безпеки напряму залежать від забезпечення захисту інформації. Це пріоритетне завдання визначено законодавством України.

Про важливість захисту інформаційної безпеки наголошується в Конституції України: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» [1].

В Законі України «Про національну безпеку України» від 21 червня 2018 зазначається: «Державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо» [2].

Законодавче визначення поняття інформаційної безпеки зафіксоване в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.»: «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [3].

На стан і перспективи інформаційної безпеки мають безпосередній вплив зовнішні та внутрішні чинники, найважливішими з яких є: 1) політична обстановка у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку країни; 4) внутрішньополітична обстановка в державі. Водночас інформаційна безпека є складною, динамічною, цілісною соціальною системою, компонентами якої є підсистеми безпеки особистості, держави і суспільства [4].

Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері визначені в Доктрина інформаційної безпеки України 2017 р [5]. Зокрема:

«здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;

поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні» [5].

Необхідність в комплексному та ефективному підході до процесу забезпечення безпеки національного інформаційного простору постійно зростає. Актуальним на сьогодні залишається визначення чітких завдань та відповідальних суб'єктів за інформаційну безпеку. Визначаючи цілі, принципи, правові складові, Доктрина має стати основою для розробки проєктів, концепцій, стратегій, цільових програм і планів дій із забезпечення інформаційної безпеки України; базою для удосконалення норм та юридичних механізмів системи захисту інформації в державі.

Діяльність органів державної влади повинна спрямовуватися на виконання конкретних завдань у цій сфері й об'єднуватися єдиною метою – надання належних умов для забезпечення інформаційної безпеки України. Узгоджена діяльність по забезпеченню інформаційної безпеки на основі єдиних правових норм сприятиме ефективному протистоянню інформаційним загрозам; попередженню, реагуванню та розслідуванню будь-яких посягань на інформаційну безпеку України.

Література

1. Конституція України // Електронний ресурс: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення 08.03.21).

2. Закон України «Про національну безпеку України» від 21 червня 2018 //Електронний ресурс:https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення 08.03.21).

3. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.» //Електронний ресурс: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення 08.03.21).

4. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України/ Юридичний науковий електронний журнал. – 2020. - № 2 // Електронний ресурс: http://lsej.org.ua/2_2020/54.pdf(дата звернення 08.03.21).

5. Доктрина інформаційної безпеки України 2017 р//Електронний ресурс: https://zakon.rada.gov.ua/laws/show/47/2017#Text(дата звернення 08.03.21).

УДК 623.618

ЛОЗА В.В.
Національний університет оборони України
імені Івана Черняховського

КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ В УМОВАХ «ІНДУСТРІЇ 4.0»

Епоха третьої промислової революції добігає кінця, сучасний світ стрімко входить в епоху четвертої промислової революції (“Індустрія 4.0”), концепцію якої вперше сформульовано як впровадження кіберфізичних систем в виробничі процеси (Ганновер, 2011). Передбачається, що ці системи об’єднаються в одну мережу, будуть зв’язуватися одна з одною в режимі реального часу, самоналаштовуватися та навчатися новим моделям поведінки. Не виключенням є і наша держава, яка запровадила вседержавну цифрову трансформацію (“діджиталізацію”). Серед проектів цифрової трансформації на наступні три роки передбачено: е-нотаріат, е-майно, е-містобудування, е-школа, е-соцзахист, е-міграція, е-лікарня, е-дозвіл тощо [1].

Саме зараз розпочинається з’єднання двох світів: виробництва та мережевих з’єднань шляхом Кіберфізичних Систем (CPS), Кіберфізичних виробничих систем (CPPS) та Інтернету речей (IoT).

Повномасштабна цифровізація, впровадження сучасних технологій, використання робототехнологій, які спрямовані на розуміння нової виробничої парадигми в епоху “Індустрії 4.0” передбачає зміну підходів до управління та адміністрування інформаційно-телекомунікаційними системами (ІТС).

Але, в той же час, масове використання в якості управляючого інструменту комп’ютеризованих компонентів, алгоритм роботи яких залежить від застосованого програмного забезпечення, породжує появу та шалене зростання кількості нових атак на ІТС, насамперед кібератак.

Сьогодення показує, що ІТС держави не інтегровані між собою або інтегровані частково. В той час як “Індустрія 4.0” передбачає, що функціона-

льні складові в рамках єдиної структури створюють загальний універсальний інформаційний простір з метою автоматизації відразу декількох процесів управління.

На даний час все більше використовується програмне забезпечення та системи аналізу на основі “хмарних” платформ. Епоха четвертої промислової революції передбачає збільшення потоків обміну даними, що виходять за межі окремо взятого відомства, організації і т.п. Тому, не виключено, що в подальшому системи моніторингу та контролю стану ІТС перейдуть на “хмарні” платформи.

Кіберзлочинці використовують наявні інструменти кібервпливу для проведення кібератак на об’єкти критичної інфраструктури держави, в першу чергу на складові сектору безпеки та оборони [2]. В умовах сучасної геополітичної обстановки актуальним на сьогодні залишається питання забезпечення безпеки, у тому числі і кібербезпеки ІТС. Саме тому на тлі російсько-української кібервійни Президент України указом № 242 від 7 червня 2016 року створив Національний координаційний центр кібербезпеки. [3]. На центр покладено відповідальність за аналіз стану кібербезпеки, готовності до протидії кіберзагрозам, фінансового й організаційного забезпечення програм і заходів із забезпечення кібербезпеки, прогнозування й виявлення потенційних і реальних погроз у сфері кібербезпеки, участь в організації й проведення міжнаціональних і міжвідомчих кібернавчань і тренінгів.

Зміни в об’єктах критичної інфраструктури держави, що підлягають першочерговому захисту, приводять до нових спроб впливу на стійкість їх функціонування та урізноманітнення способів та шляхів впливу. Новому класу загроз, а саме кіберзагроз, повинен протистояти новий клас систем забезпечення безпеки, а саме: система кіберзахисту [4].

Більшість відомих нам систем виявлення атак (СВА), що застосовуються для моніторингу безпеки ІТС, основані на використанні правил та сигнатур, за допомогою яких проводиться аналіз вектору вхідних даних та на основі чого робиться висновок про наявність чи відсутність атаки. При найменшому відхиленні сигнатури атаки от сигнатури чи правила, що зазначено в базі даних, ця атака не виявляється. Тому із-за великого різновиду атак звичайні СВА не завжди можуть забезпечити ідентифікацію атаки. Одним із варіантів рішення цієї проблеми може бути використання нейромереж.

Відомо, що якість виконання завдань управління залежить від можливості ІТС зберігати задану стійкість функціонування на протязі визначеного часу виконання своїх основних функцій в межах, встановлених нормативними вимогами, в умовах впливу різних факторів. Адже в епоху “Індустрії 4.0” (зі збільшенням кількості з’єднань та використанням стандартних та новітніх протоколів обміну інформацією), подальшого стрімкого ро-

звитку цифрових технологій поряд із добре відомими показниками стійкості функціонування ІТС (живучість, надійність, завадозахищеність, кіберзахищеність) з'являється ще один: здатність ІТС до трансформації у різних умовах обстановки, у тому числі і під дією кібервпливу.

Застосування нового показника для оцінювання стійкості функціонування ІТС, у т.ч. і в умовах кібервпливу, який можна характеризувати такими взаємопов'язаними між собою функціями як реконфігуративна, реорганізаційна, реконструктивна, диверсифікаційна та репродуктивна, потребує на даний час розроблення методик його оцінювання із застосуванням саме нейромережевої технології.

Література

1. Інтернет посилання: https://kp-rda.gov.ua/news/1613725514.

2. Закон України від 21.06.2018 №2469-VIII "Про національну безпеку України".

3. Указ президента України №96/2016 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України".

4. Закон України від 05.10.2017 №2163-VIII "Про основні засади забезпечення кібербезпеки України".

УДК 342.9

Олійник І.О.
Національна академія Служби безпеки України

ЗАГАЛЬНІ ПРОБЛЕМИ ЗАХИСТУ КІБЕРНЕТИЧНОГО ПРОСТОРУ УКРАЇНИ

Актуальність проблем захисту кібернетичного простору зумовлена тим, що за останній час значно зросла кількість суспільно небезпечних дій в кіберпросторі України, а саме спрямованих на нанесення шкоди об'єктам критичної інфраструктури країни. Створення провокацій, втручання у процеси роботи для дестабілізації кібернетичного простору, виведення з ладу органів керування все це є кібернетичні загрози які розвиваються, модифікуються кожного дня. Тому наша система кіберзахисту повинна також покращуватись для ефективної протидії усім агресорам.

Значну увагу питанню дослідження захисту кібернетичного простору приділили такі вітчизняні вчені, як Шеломенський В., Грицюк Ю., Корченко О., Шлемко В., Мартинюк В., Бурячок В.

Кібербезпека - це практика захисту мереж, систем та будь-якої іншої цифрової інфраструктури від зловмисних атак. Очікується, що у світі до 2023 року збитки від кіберзлочинності перевищать колосальних 6 трильйонів доларів, недарма банки, технологічні компанії, лікарні, державні уста-

нови та майже кожен інший сектор інвестують в інфраструктуру кібербезпеки, щоб захистити свою ділову практику та мільйони клієнтів, яким довіряють їхні дані. Яка найкраща стратегія кібербезпеки? Потужна інфраструктура безпеки включає безліч рівнів захисту, розподілених по комп'ютерах, програмах та мережах компанії. Оскільки кібератаки відбуваються кожні 14 секунд, брандмауери, антивірусне програмне забезпечення, антишпигунське програмне забезпечення та засоби управління паролями повинні працювати в гармонії, щоб перехитрити напрочуд творчих кіберзлочинців. Якщо так багато на карту поставлено, не гіперболічно думати, що інструменти та експерти з кібербезпеки виступають як остання лінія захисту між нашою найважливішою інформацією та цифровим хаосом.

Тобто, створення покращення наявних умов належного упорядкування взаємозв'язків між суб'єктами забезпечення кібернетичної безпеки, засобами та методами, що ними використовуються, а також відповідних взаємопов'язаних правових, організаційних і технічних заходів, що ними здійснюються, дозволяє підвищити ефективність системи кібернетичної безпеки. Розбудова ефективної системи кібернетичної безпеки в Україні вимагає вирішення таких питань організаційного характеру, як:

– чітке визначення функцій суб'єктів забезпечення кібернетичної безпеки та розподілу повноважень між ними;

– забезпечення належної координації діяльності як загальних суб'єктів забезпечення кібернетичної безпеки, так і відповідних спеціальних суб'єктів;

– розробка та впровадження найсучасніших підходів, форм і методів забезпечення кібернетичної безпеки;

– запровадження дієвих стимулів для залучення до такого роду діяльності фахівців високого рівня кваліфікації.

До основних напрямів удосконалення організаційного забезпечення системи кібернетичної безпеки України слід віднести створення сприятливих зовнішньополітичних умов для прогресивного розвитку національного сегменту кіберпростору та забезпечення повноправної участі України в загальноєвропейській та регіональних системах кібернетичної безпеки;

Головне це зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби у кіберпросторі з проявами організованої злочинності та кібертероризму. Найлегше довести потрібність можна лише на прикладі вірусу Petya, він був лише черговим фрагментом програми-вимагателя, коли він почав циркулювати через фішингспам у 2016 році. Його головна претензія на славу полягала в тому, що вона зашифрувала головний запис завантаження заражених машин, ускладнюючи користувачеві доступ до своїх файлів. Потім раптово в червні 2017 року почала поширюватися набагато більш

вірулентна версія шкідливого програмного забезпечення. Він досить відрізнявся від оригіналу, що його охрестили NotPetya. Він спочатку розповсюджувався за допомогою компрометованого українського бухгалтерського програмного забезпечення та поширювався тим самим експлойтом EternalBlue, що задало значних збитків інфраструктури країни.

Узагальнюючи те що сьогодні реальні прояви кібератак на інформаційні ресурси України можуть призвести до порушень функціонування інформаційно-телекомунікаційних систем як звичайної, так і критичної інфраструктури, які безпосередньо впливають на стан національної безпеки і оборони держави. У зв'язку із цим наявні загрози вимагають впровадження державою комплексних заходів щодо забезпечення її кібербезпеки.

Література

1. Кібербезпека України проблеми та перспективи їх подолання . URL: https://core.ac.uk/download/pdf/233854664.pdf.

2. Тренди кібератак. URL: https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html.

3. Кіберпростір та аналіз кібератак .URL: https://www.sciencedirect.com/topics/computer-science/cyber-attack.

4. Cybersecurity Statistics and Trends for 2021 URL: https://www.varonis.com/blog/cybersecurity-statistics/.

УДК 343.98

Омельян О.С.
Національна академія Служби безпеки України

ЩОДО ПРОБЛЕМИ ФОРМУВАННЯ ПОНЯТІЙНО-ТЕРМІНОЛОГІЧНОГО АПАРАТУ У СФЕРІ КІБЕРБЕЗПЕКИ

Важливу роль у нормативно-правовому регулюванні забезпечення кібербезпеки в державі відіграє термінологічний апарат. Терміни повинні бути чіткі, однозначні та зрозумілі.

На даний час в Україні використовується декілька законодавчо визначених термінів, які, фактично, означають одне і те саме або є дуже близькими за змістом:

- електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі, мережі електрозв'язку – ст. 361 КК України [1];
- інформаційна (автоматизована) система, телекомунікаційна система, інформаційно-телекомунікаційна система – Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [2];

- комунікаційна система, технологічна система (яка є автоматизованою або автоматичною системою) – Закон України «Про основні засади забезпечення кібербезпеки України» [3];

- електронна комунікаційна мережа, технічні засоби електронних комунікацій – Закон України «Про електронні комунікації» [4].

І це не враховуючи термінів, закріплених у підзаконних нормативних актах (маються на увазі Державні стандарти України, нормативні документи технічного захисту інформації тощо). Наприклад, «система автоматизована» (ДСТУ 2226-93) [5] та «автоматизована система керування технологічними процесами» (ДСТУ 2709-94) [6].

На нашу думку, таке різноманіття термінів може обумовити плутанину. Поглиблює проблему й те, що вказані терміни розміщені в різних нормативних документах. Тому актуальною є уніфікація зазначених вище нормативних документів. При цьому серед рівнозначних термінів слід обрати один, який найбільш відповідає вимогам сьогодення, а також визначити співвідношення згаданих термінів між собою. Доцільним вбачається навести усі терміни в одному нормативному документі, наприклад, привести у відповідність до сучасних вимог та потреб ДСТУ 2226-93 «Автоматизовані системи. Терміни і визначення», удосконалити вже наведені у ньому терміни та доповнити стандарт новими.

Крім того, доречним є таке становище, коли і в законах, що регулюють певні соціальні відносини, і в кримінальному законі, який ці відносини охороняє, об’єкт правової охорони сформульований однаково. Тому існують підстави розширити уніфікацію зазначених вище законодавчих актів у частині використовуваних в них термінів також і на відповідні статті КК України.

Наприклад, якщо розглянути ст. 361 КК України, то в розрізі описаних в її диспозиції протиправних дій варто згадати закріплені у Законі України «Про основні засади забезпечення кібербезпеки України» формулювання кібератаки, яке в цілому, на нашу думку, є вдалим:

«кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту».

Зокрема, у зазначеному формулюванні кібератаки виділено основні властивості інформації, що підлягають захисту – конфіденційність, доступність, цілісність. Цілі кібератаки доповнено проміжною ланкою – отримання контролю над системою задля використання її ресурсів під час здійснення подальших злочинних дій в кіберпросторі.

Вважаємо, що наведене визначення доцільно б передбачити у примітці до ст. 361 КК України, дія якої поширюватиметься на інші статті «комп'ютерного» блоку КК України.

Вирішення питань узгодженості норм кримінального закону з нормами інших нормативно-правових актів стосовно забезпечення кібербезпеки сприяло б підвищенню ефективності його застосування.

Література

1. Кримінальний кодекс України: Закон України від 5 квітня 2001 року № 2341-III. База «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

2. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР. База «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

3. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року №2163-VIII. База «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

4. Про електронні комунікації: Закон України від 16 грудня 2020 року №1089-IX. База «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

5. Автоматизовані система. Терміни і визначення: Державний стандарт України 2226-93.

6. Автоматизовані системи керування технологічними процесами. Метрологічне забезпечення. Основні положення: Державний стандарт України 2709-94.

УДК 355.40:356

Петренко К.М.
Національний університет оборони України
імені І. Черняховського

ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ ДЕРЖАВІ У ВОЄННІЙ СФЕРІ

На сьогодні світовий геополітичний простір та внутрішньодержавні відносини формуються в умовах інформаційного протиборства. Для нашої держави ця проблема особливо актуальна зважаючи на певну невизначеність геополітичного статусу, політичну нестабільність, нестійкість вітчиз-

няного інформаційного простору, Україна перебуває під систематичним інформаційним тиском. В умовах впливу Росії на Україну, підбурювання, організації та всебічного забезпечення збройного протистояння на Сході нашої держави, проявляється нова тенденція ведення Росією воєнних дій. Водночас всі ці заходи супроводжуються цілеспрямованою потужною інформаційною кампанією. В часи інтенсивного розвитку інформаційних технологій, наявності глобальних інформаційних мереж і не менш глобалізованих засобів масової інформації, складова "інформаційного супроводу" у гібридних війнах має надзвичайно важливе, якщо не вирішальне, значення. У цих умовах гостро постає проблема захисту національного інформаційного простору. Враховуючи викладене, пошук шляхів надійного виявлення, аналізу та оцінюванню інформаційних загроз та протидії їм є актуальним науковим та практичним завданням.

Комплексна методика оцінювання інформаційних загроз державі у воєнній сфері базується на показниках, які характеризують інформаційний вплив для кожного напряму, якими є:

рівень інтенсивності негативного інформаційного впливу;

тривалість негативного інформаційного впливу;

поширеність джерел інформаційного впливу;

масштаб об'єктів інформаційного впливу.

Зазначені показники враховують комплекс завдань - від виявлення ознак негативного інформаційного виливу до визначення переліку конкретних заходів негативного інформаційного впливу.

Удосконалена методика дає змогу виробити шляхи зниження рівня ІЗ державі у воєнній сфері та практично застосувати їх, а саме:

в органах військового управління та органах державної влади, на які покладено завдання виявлення, аналізу та оцінювання інформаційних загроз національній безпеці України, зокрема для розробки та супроводження паспортів воєнних загроз національній безпеці;

в органах державної влади, які займаються розробкою законодавчий та нормативних документів [1,2].

Література

1. Концепція забезпечення інформаційної безпеки МО України і ЗС України. https://www.mil.gov.ua/content/mou_orders/612_nm_2017.

2. Дослідження можливих шляхів удосконалення системи забезпечення інформаційної безпеки Міністерства оборони та збройних сил України :звіт про НДР (закл.) / Кафедра застосування інформаційних технологій та інформаційної безпеки ; керівн. С. А. Микусь ; викон. :О. В. Войтко [та ін.]. – К., 2019. – 201 с. - Інв. № 9535 у НУОУ.

УДК 351.86(477)
Прогонюк М.С.
Благодарний А.М.
доктор юридичних наук, старший науковий співробітник,
Національна академія Служби безпеки України

УДОСКОНАЛЕННЯ ПРАВОВОЇ РЕГЛАМЕНТАЦІЇ ДЕРЖАВНО-ПРИВАТНОЇ ВЗАЄМОДІЇ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

З розвитком технологій людство в цілому й окремі держави, зокрема, займають нові простори для діяльності. Раніше це проявлялось у географічному аспекті, однак, наразі важливу роль відіграють нові сфери, на які покладаються певні функції. Одним із таких новоутворень, що відрізняється своїми специфічними рисами, є кіберпростір. Водночас, новітні простори передбачають й появу нових загроз, а, відповідно, й пошук шляхів, способів та методів їх попередження, виявлення та усунення.

Природно, що з початком повноцінного функціонування кіберпростору, найуразливішими стали традиційні складові національної безпеки, зокрема об'єкти критичної інфраструктури. Однак на сьогодні, незважаючи на прийняття ряду нормативно-правових актів, що регулюють цю сферу, вирішення питання взаємодії державного та приватного секторів з метою забезпечення кібербезпеки потребує подальшого удосконалення. Особливо гостро це виявляється під час захисту об'єктів критичної інфраструктури.

Чинним законодавством термін кібербезпека визначається 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 [1].

Враховуючи комплексність і відносну новизну діяльності щодо забезпечення кібербезпеки, вона потребує застосування всіх наявних засобів та залучення усіх доступних сил. Це відобразилось й у принципах, закріплених на законодавчому рівні: державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема, шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проєктів, навчання та підвищення кваліфікації кадрів у цій сфері [1; 2]. Однак, поряд з нормативно-правовим регулюванням не менш актуальним є питання практичної реалізації заходів, спрямованих на захист об'єктів критичної інфраструктури у кіберпросторі.

Об’єкти критичної інфраструктури вирізняються саме своїм вагомим значенням для економіки та промисловості, функціонування суспільства та безпеки населення, а отже забезпечення складових її безпеки, зокрема й у кіберпросторі, однаково важливе як для приватного так і для державного сектору. Така взаємодія двох вказаних секторів зумовлена демократичними засадами вітчизняного державотворення, адже під безпосереднім (за формою власності і можливостями адміністративно-правового впливу) контролем держави перебуває лише частина об’єктів критичної інфраструктури [3, с. 52].

Незважаючи на визначення форм, у яких повинна реалізовуватись державно-приватна взаємодія у сфері забезпечення кібербезпеки, її практична реалізація потребує удосконалення. Перш за все, досі чітко не визначено характер такої взаємодії, як вона співвідноситься з державно-приватним партнерством.

По-друге, наразі не встановлено мінімальну частку участі у проєкті забезпечення кібербезпеки приватного суб’єкта (наприклад, у деяких європейських країнах мінімальна частка приватного фінансування становить 25%) [3, с. 54]. Це дозволяє приватним партнерам перекладати більшу частину відповідальності та зусиль на державний сектор. Варто додати, що великі ризики для іноземних інвесторів в Україні також не сприяють як державно-приватній взаємодії у вказаній сфері, так й міжнародному співробітництву у цілому.

Також, належним чином не вирішено питання координації та управління в рамках державно-приватної взаємодії, зокрема, який з секторів, не говорячи вже про конкретний орган, може приймати управлінські рішення, який їх статус для суб’єктів взаємодії.

Отже, на сьогодні стан нормативно-правового забезпечення кібербезпеки об’єктів критичної інфраструктури кращий ніж декілька років тому, хоча і потребує подальшого вдосконалення. Водночас, у контексті забезпечення безпеки людини, суспільства, держави у кіберпросторі, особливої актуальності набуває питання реалізації вже закріплених норм. Наявні проблеми повинні бути вирішені з урахуванням як вітчизняної досвіду практичного діяльності у цій сфері так і позитивних здобутків інших держав.

Література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. URL: http://zakon.rada.gov.ua/laws/show/2163-19.

2. Про Стратегію кібербезпеки України : Указ Президента № 96/2016 від 15.03.2016. URL: https:// zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 02.09.2019).

3. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова. – К. : НІСД, 2018. – 84 с.

УДК 327.57
Прозоров А.Ю.
кандидат юридичних наук,
Національна академія Служби безпеки України

ОКРЕМІ АСПЕКТИ СПІВПРАЦІ УКРАЇНА-НАТО У СФЕРІ З ЗАХИСТУ ІНФОРМАЦІЇ

З позицій інформаційної безпеки вся інформація у світі поділяється на загальнодоступну і ту, доступ до якої з тих чи інших причин обмежується. В українській національній практиці така інформація має назву «інформація з обмеженим доступом». В англомовній традиції їй відповідає поняття «вразлива інформація» (SENSITIVE), тобто інформація, яка вразлива до загроз, що виникають у зв'язку з несанкціонованим доступом до неї, і тому потребує захисту або хоча б обмеження доступу до неї. Саме таке визначення прийнято в НАТО і країнах − членах Альянсу [].

Як слушно зазначає Болдир С.В., у стандартах безпеки НАТО та ЄС, а також нормативній базі більшості країн-членів цих міжнародних організацій відсутні поняття «державна таємниця», «службова інформація», натомість передбачено застосування єдиного терміну для позначення відомостей з еквівалентними ступенями обмеження доступу, а саме – «classified information», прямим перекладом якого є «класифікована інформація» (саме у такому написанні вказаний термін поширено використовується в україномовних ресурсах) [2].

Стандарти охорони інформації НАТО з обмеженим доступом, обов'язкові для виконання, погоджено країнами НАТО в Політиці безпеки НАТО, С-М(2002)49, а також підтримуючих директивах (зі змінами).

Документ С-М(2002)49 проголошує пять основних принципів політики безпеки НАТО: «Принцип широти» («Breadth»), «Принцип глибини» («Depth»), «Принцип централізації» («Centralization»), «Принцип управління доступом» («Controlled Distribution»), «Принцип персонального контролю» («Personnel Controls») [3].

Адміністративні домовленості щодо охорони інформації з обмеженим доступом між Урядом України та організацією Північноатлантичного договору (надалі – Домовленості) є похідними від вищезгаданих нормативних документів, застосовуються для охорони та поводження з інформацією НАТО з обмеженим доступом, переданої до України, та з інформацією України з обмеженим доступом, переданої до НАТО [4].

Аналіз зазначеного документу, на нашу думку, дає підстави дійти висновку про відповідність його вищезгаданим п'яти принципам політики безпеки НАТО.

Так, в статті 4 «Допуск та надання доступу до інформації з обмеженим доступом» Домовленостей використано «Принцип широти» (Breadth) через зобов'язання Сторін (України та НАТО) регулювати доступ до усіх видів чутливої інформації однаковим способом, незалежно від того, чи належить вона НАТО, чи Україні [4].

Відповідно до «Принципу глибини» (Depth) в Домовленостях запроваджена система поділу інформації з обмеженим доступом за чутливістю. Грифи обмеження доступу використовуються для визначення чутливості інформації з обмеженим доступом і, відповідно, встановлення процедур і правил, що застосовуються для її охорони та поводження з нею. Сторони позначають свою власну інформацію з обмеженим доступом згідно зі своїми відповідними системами ступенів обмеження доступу. Для цілей цих Домовленостей грифи обмеження доступу України та НАТО співвідносяться таким чином:

- в Україні – цілком таємно, що відповідає в НАТО – NATO SECRET;
- в Україні – таємно, що відповідає в НАТО – NATO CONFIDENTIAL;
- в Україні – для службового користування, що відповідає в НАТО – NATO RESTRICTED [4].

Згідно з «Принципу централізації» (Centralization) в Домовленостях визначено орган безпеки, а саме Служба безпеки України, що забезпечує впровадження мінімальних стандартів охорони та поводження з інформацією з обмеженим доступом, обмін якою здійснюється між Україною та НАТО.

У 1955 році в НАТО було засновано Бюро безпеки, що в подальшому перетворене у орган безпеки під назвою Офіс безпеки НАТО (NOS), що організовує координацію з питань інформаційної безпеки в НАТО. Офіс безпеки НАТО інформує національні уряди щодо застосування принципів і стандартів та проводить моніторинг національних систем з метою гарантування захисту інформації з обмеженим доступом. СБ України та Офіс безпеки НАТО сприяють проведенню взаємних перевірок з метою досягнення впевненості, що передана будь-якій Стороні інформація належним чином захищена [4].

Відповідно до «принципу персонального контролю» (Personnel Controls) перед наданням особі доступу до інформації з обмеженим доступом зі ступенем «Таємно»/«NATO CONFIDENTIAL або «Цілком Таємно»/NATO SECRET, вона повинна пройти процедуру перевірки, не менш жорсткої, ніж передбачена стандартами, викладеними у Політиці безпеки НАТО C-M(2002)49 та її підтримуючих директивах (зі змінами), для встановлення її надійності та рівня довіри до неї. Якщо результат процедури перевірки є позитивним, органом безпеки надається особі допуск та оформлюється Сертифікат особового допуску НАТО (далі – сертифікат НАТО) згідно з формою, визначеною в підтримуючій директиві

AC/35-D/2000-REV7 (зі змінами). Поряд з цим, відповідно до Домовленостей встановлюються процедури, які гарантують, що, у разі виявлення негативної інформації стосовно особи, органом безпеки або компетентним національним органом приймається рішення щодо доцільності подальшої дії наданого їй допуску [4].

Згідно з «Принципом управління доступом» (Controlled Distribution) вся інформація, обмін якою здійснюється на підставі Угоди про безпеку, повинна використовуватися виключно у службових цілях. Така інформація надається лише особам, які потребують доступу до неї за умовами своєї службової діяльності, та пройшли перевірку знань відповідних процедур безпеки; крім того, доступ до інформації з грифом «Таємно» або NATO CONFIDENTIAL і вище надається лише особам, які мають відповідний допуск до інформації з обмеженим доступом (далі – допуск). Допуск для доступу до інформації з грифом обмеження доступу «Для службового користування»/HATO RESTRICTED не вимагається. При цьому така інформація надається лише особам, які потребують доступу до неї за умовами своєї службової діяльності та пройшли перевірку знань щодо їх обов'язків стосовно охорони та поводження з інформацією з грифом обмеження доступу «Для службового користування»/HATO RESTRICTED [4].

Домовленості фактично започаткували процес імплементації стандартів НАТО у сфері захисту інформації у національне законодавство України. Вперше п'ять принципів політики безпеки НАТО знайшли повне відображення у українському правовому акті. Подальший розвиток співпраці України та НАТО з розроблення та використання стандартів захисту інформації дозволить вдосконалити національне законодавства в контексті запровадження ефективних правових заходів протидії загрозам національним інтересам України в інформаційній сфері, а саме у кіберпросторі.

Література

1. Вікіпедія «Класифікована інформація» [Електронний ресурс] / Класифікована інформація. – Режим доступу: http://uk.m.wikipedia.org/wiki/Класифікована_інформація.

2. Перспективи реформування системи охорони державної таємниці та службової інформації «Інформація і право» № 4(23)/2017 с. 79-85.

3. Al. S. Roberts Nato security of information policy and the entrenchment of State Secrecy. Reports Basic Newsletter on Internal International Security October 2003 Nb;.

4. Адміністративні домовленості щодо охорони інформації з обмеженим доступом між Урядом України та Організацією Північноатлантичного договору : Закон України від 24.05.17 р. № 2068-VIII – Режим доступу : http://zakon5.rada.gov.ua/laws/show/950_035-16.

УДК 343.592
Решетніков Д.І.
Національна академія Служби безпеки України

КІБЕРЗЛОЧИННІСТЬ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

Інформаційна безпека є сферою у складі національної безпеки поряд із іншими сферами безпеки: воєнною, зовнішньополітичною, державною, економічною, екологічною, громадською безпекою і порядком та кібербезпекою (п. 3 ч. 1 ст. 1, ч. 4 ст. 3 Закону України "Про національну безпеку України"). У складі інформаційної безпеки є інформаційно-психологічна та інформаційно-телекомунікаційна сфери. Контррозвідувальний захист кібербезпеки та інформаційної безпеки держави покладено на Службу безпеки України (ст. 19 зазначеного Закону України). Закон України "Про контррозвідувальну діяльність" визначає завдання із контррозвідувального забезпечення інформаційного, науково-технічного потенціалу та національної системи зв'язку (п. 2 ч. 1 ст. 6). Зважаючи на рівну юридичну силу двох законів щодо повноважень СБУ обома зазначеними законодавчими актами, контррозвідувальний захист інформаційної безпеки держави та її кібербезпеки є повноваженням СБУ, що реалізується засобами контррозвідувальної діяльності. Остання, за визначенням (ст. 1 Закону України "Про контррозвідувальну діяльність") є спеціальним видом діяльності ***у сфері забезпечення державної безпеки,*** яка здійснюється з використанням системи заходів, спрямованих на попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, розвідувальним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також *організацій, окремих груп та осіб на інтереси України*. Видається цілком очевидним, що кримінальні правопорушення, об'єктом, предметом або засобом вчинення яких є інформація та засоби її обробки, елементи кібернетичної інфраструктури тощо можуть набувати форм протиправного посягання на інтереси України (зокрема, в інформаційній сфері та у сфері кібербезпеки) та одночасно бути джерелом [кримінальних] загроз безпеці України. Закон припускає можливість "заведення за матеріалами контррозвідувальної діяльності оперативно-розшукової справи" та "притягнення особи до кримінальної відповідальності, в тому числі і за кордоном, за дії, що були підставами для заведення контррозвідувальної справи; (п.п. 5,6 ч. 10 ст. 8 Закону України "Про контррозвідувальну діяльність"). Вказане обумовлює доцільність у роботі з виявлення загроз [інформаційній] безпеці України враховувати і *кримінальні загрози*.

В рамках Угоди між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво (ратифіковано Законом

№ 2129-VIII від 12.07. 2017), здійснюється обмін інформацією, спеціальними знаннями, загальними зведеннями, результатами стратегічного аналізу, інформацією щодо процедур кримінальних розслідувань, інформацією про методи запобігання злочинності тощо (ст.ст. 4, 10, 12 Угоди). Тому правомірним і доцільним є використання Україною в особі визначеного Угодою кола компетентних органів результатів стратегічного аналізу, проведеного Європолом. Зокрема, окрему увагу слід приділити матеріалам щорічного дослідження "IOCTA" - Internet Organised Crime Threat Assessment, яке проводиться підрозділом Європолу – Європейським центром кібербезпеки. У промо-ролику до видання 2020 року зазначено: "Ми живемо у цифрову епоху. Злочинці - також". З огляду на євроінтеграційні прагнення України, збільшення міграційних потоків та міждержавних зв'язків, та зважаючи, що із інформаційними технологіями в нашу державу імпортується також і комп'ютерна злочинність, результати дослідження мають постійно враховуватися під час визначення ризиків національної безпеки України [1].

На думку фахівців Європолу, реалізовані зі зростаючою повагою до приватності криптовалюти та криптосервіси полегшують, в тому числі, платежі у численних формах кіберзлочинів; домінуючою є загроза вимагання «викупу» за не оприлюднення даних, зібраних хакерами щодо своїх «жертв»; зростає кількість шахрайства, пов'язаних із онлайн-інвестуванням; площадки електронної торгівлі та зашифровані комунікаційні платформи надають додатковий вимір для незаконних оборудок, що вчиняються у «темному Інтернеті» (Dark web) [2]. Актуальними також є загрози вчинення в Інтернеті аморальних дій стосовно дітей та їх сексуальної експлуатації.

Наразі, СБУ залучається до напрацювання Стратегії кібербезпеки України та Стратегії інформаційної безпеки (розробляються на виконання п. 66 Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392/2020 та ст. 31 Закону України «Про національну безпеку України». Вони мають включати оцінку кримінальних загроз із урахуванням ризиків, та загроз, визначених Європолом.

Література

1. https://www.europol.europa.eu/iocta-report.

2. Internet Organised Crime Threat Assessment / *Europol*. 2020 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

УДК 004.056.5
Саакянц І.О.
Національна академія Служби безпеки України

МІЖНАРОДНІ СТАНДАРТИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА МОЖЛИВОСТІ ЇХ ЗАСТОСУВАННЯ ДЛЯ ВДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В СЛУЖБІ БЕЗПЕКИ УКРАЇНИ

В сучасному світі інформація набуває нового значення, перетворюючись на важливий ресурс, не менш, а часто і більш вартісний, ніж матеріальні ресурси. До того ж інформація сьогодні визнається головною цінністю цивілізації й отримує статус домінанти. У зв'язку з цим питання забезпечення інформаційної безпеки стає дедалі актуальнішим. Зазначимо, що поняття інформаційної безпеки є досить багатогранним, ми ж пропонуємо зупинитися на тих його аспектах, які пов'язані з захистом інформації, що в міжнародній практиці трактується як забезпечення її конфіденційності, цілісності та доступності [1].

Сьогодні практично кожна організація (підприємство, установа) намагається захистити інформацію, якою вона володіє або розпоряджається. З цією метою вживаються відповідні заходи: розробляються стратегії та плани, створюються спеціалізовані підрозділи, придбається програмне та апаратне забезпечення тощо. Проте без єдиної системи управління інформаційною безпекою усі ці заходи перетворюються на хаотичну сукупність не пов'язаних між собою дій, а їх ефективність неухильно знижується.

У зв'язку з цим багато організацій в основу заходів із забезпечення інформаційної безпеки поклали міжнародний стандарт ISO/IEC 27001:2013 «Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою – Вимоги» (далі – ISO/IEC 27001), який був випущений Міжнародною організацією зі стандартизації спільно з Міжнародною електротехнічною комісією у 2005 році та зазнав ревізії у 2013 році. Стандарт містить вимоги щодо створення, впровадження, підтримання та постійного вдосконалення системи управління інформаційною безпекою в рамках організації [1]. Якщо організація запроваджує у свою діяльність стандарт, це означає, що вона «застосовує систематичний підхід до виявлення, оцінки та управління ризиками інформаційної безпеки» [2].

Стандарт вимагає, щоб система управління інформаційною безпекою забезпечувала: постійне вивчення ризиків інформаційної безпеки організації з урахуванням загроз, вразливостей та їх можливих наслідків; розробку та впровадження комплексу засобів контролю за інформаційною безпекою або інших форм управління ризиками з метою виявлення неприйнятних ризиків; всебічний та безперервний процес управління, який би гарантував,

що контроль за інформаційною безпекою продовжує відповідати потребам організації [1].

ISO/IEC 27001 містить вимоги щодо оцінки та управління ризиками інформаційної безпеки, адаптовані до потреб організації. Вимоги, викладені у стандарті, можуть бути застосовані до всіх організацій, незалежно від їх типу, розміру чи характеру їх діяльності [1]. Враховуючи, що положення ISO/IEC 27001 є універсальними та стосуються як суб'єктів приватного, так і державного сектору, Служба безпеки України (далі – СБУ) може покласти принципи та підходи стандарту в основу подальшої розбудови власної системи управління інформаційною безпекою.

Очевидно, що співробітники СБУ зобов'язані забезпечувати належний захист інформації під час її створення та обробки (зокрема, збирання, перетворення, зберігання, знищення, передавання тощо), і роблять це на постійній основі. Однак недостатнє матеріально-технічне забезпечення та відсутність єдиної системи управління інформаційною безпекою, яка б постійно розвивалася та адаптувалася до нових умов, можуть призводити до порушення безпекових вимог (наприклад, використання мобільних телефонів в службових приміщеннях, що необхідно для роботи, за певних обставин може призвести до витоку інформації).

На наш погляд, було б корисним враховувати вимоги ISO/IEC 27001 при організації захисту інформації в СБУ, зокрема в процесі інформаційно-аналітичної діяльності, адже стандарт пропонує комплексний та всебічний підхід до забезпечення інформаційної безпеки. ISO/IEC 27001 не тільки встановлює вимоги щодо створення систем управління інформаційною безпекою, але передбачає постійне вдосконалення та верифікацію таких систем, а також допомагає забезпечувати інформаційну безпеку «під прямим і постійним контролем управління» [1]. Наголосимо, що сам стандарт теж розвивається відповідно до змін, які відбуваються в інформаційній сфері, та з урахуванням досвіду його застосування, а його остання версія суттєво відрізняється від версії 2005 року. Таким чином, СБУ, звернувшись до цього стандарту, отримає можливість скористатися з передових міжнародних практик у галузі захисту інформації.

Цілком зрозуміло, що СБУ з міркувань безпеки не може пройти через процедуру сертифікації на предмет відповідності стандарту ISO/IEC 27001, але вона може розвивати власну комплексну систему захисту інформації з урахуванням принципів та рекомендацій стандарту. При перегляді нормативної бази з питань функціонування відомчих інформаційно-телекомунікаційних систем та організації інформаційно-аналітичної діяльності в СБУ доцільно враховувати вимоги ISO/IEC 27001. Також потрібно звернути увагу на підвищення рівня обізнаності співробітників СБУ в питаннях інформаційної безпеки.

Література

1. BS ISO/IEC 27001:2013 (BS 7799-2:2013) *Information technology. Security techniques. Information security management systems. Requirements*. ISO/IEC. 2013.

2. European Union Agency for Cybersecurity. *The Need for ISMS.* URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/need (дата звернення 05.03.2021).

УДК 323.21

Савіцька В.І.
Гоц О.В.
Національна академія Служби безпеки України

ДЕРЖАВНА СТРАТЕГІЯ ДЕОКУПАЦІЇ КРИМУ: ЩО БУДЕ ДАЛІ?

Росія окупувала Крим у 2014 році. 16 березня 2014 року на території Криму та Севастополя відбувся невизнаний більшістю країн світу «референдум», в результаті якого Росія анексувала Крим. Ні Україна, ні Європейський Союз, ні США не визнали результатів голосування на "референдумі", але сама Росія називає це "відновленням історичної справедливості".

Примусова окупація та незаконна анексія Криму- Російською Федерацією закінчилася порушенням прав людини, мілітаризацією Кримського півострова та фактичним знищенням основних принципів глобальної безпеки. У той же час дії Росії в Криму, разом з необхідністю відповісти на першу незаконну анексію в Європі після закінчення Другої світової війни, стали справжнім викликом українській політичній та адміністративній еліті і владі, особливо на тлі російської агресії в Донецькій та Луганській областях, а також намагання зробити Крим своєю частиною. Окупація та анексія Криму призвели до погіршення ситуації з правами людини.

На початку січня цього року ЄСПЛ визнав, що контроль Росії над окупованим Кримом розпочався ще до незаконної анексії. Фактичний контроль Росії над окупованим півостровом Крим розпочався не пізніше 27 лютого 2014 року. Для вирішення ситуації, враховуючи обмежений вплив України на процеси в Криму, уряд склав стратегію деокупації та реінтеграції тимчасово окупованої території Автономної Республіки Крим та міста Севастополя. Ця стратегія передбачає заходи в галузі економіки, торгівлі, інформації, освітньої політики, транспорту та інших для реагування на порушення прав і свобод людини, а також на порушення прав кримських татар в окупованому Росією Криму.

Першим питанням, яке було розглянуто, був проект державної стратегії деокупації та реінтеграції тимчасово окупованих територій Автономної Республіки Крим та міста Севастополя. Перше питання розглядалось у закритому режимі. Встановлення миру та деокупація усіх територій України

були одним із пріоритетів передвиборчої кампанії Володимира Зеленського. Стратегія реінтеграції тимчасово окупованих територій та розвитку міцної системи національної безпеки та оборони обговорювалася на засіданні під головуванням Президента України.

Зокрема, було сказано, що держава вже розробляє ефективні інструменти безпечної реінтеграції тимчасово окупованих територій. Цей процес включатиме створення міжнародної коаліції для підтримки зусиль нашої держави щодо відновлення територіальної цілісності на всіх переговорних майданчиках, відновлення міжнародних переговорів про деокупацію Криму, реінтеграцію дітей та молоді, розробку механізмів вирішення житлових питань, забезпечення інформації суверенітет та доступ до адміністративних послуг для жителів тимчасово окупованих територій. Сторони також обговорили питання зміцнення української армії, яка функціонуватиме відповідно до принципів, норм та стандартів держав-членів НАТО.

Президент доручив міністру оборони Андрію Тарану розробити чіткий план забезпечення Збройних Сил зразками нової та якісно відремонтованої техніки та терміни побудови професійної армії. Також Глава держави наполягає на забезпеченні всіх категорій військовослужбовців Збройних Сил високими зарплатами та розробці чіткої програми забезпечення житлом усіх військовослужбовців, які цього потребують.

Тож, чи є сенс у просуванні Кримської стратегії деокупації? Однозначно ТАК!

Перша теза дуже проста: слід визнати, що будь-які переговори з Кремлем щодо Криму чи Донбасу приречені на провал, а політиків, які говорять про протилежне, слід розглядати як безвідповідальних наслідувачів.

Друга теза: українці повинні розуміти, що для повного відновлення суверенітету та територіальної цілісності України знадобиться багато часу ... що це стане можливим лише після зміни влади в Росії і коли новий російський уряд або перегляне свої політичні пріоритети, або зіткнеться величезна економічна та політична криза. Путін ніколи не здасть Крим або Донбас; навпаки, він готовий захопити нові території України.

Третя теза: протягом цього тривалого періоду очікування все буде залежати від самих українців, а точно не від росіян чи Заходу. Громадяни України повинні навчитися відповідально голосувати за справжніх державних діячів, а не за колабораціоністів чи популістів чи за політиків, які на все погоджуються. Українці повинні навчитися відмовлятися від олігархічної пропаганди і не вірити у спрощені способи вирішення конфлікту з Росією. Крім того, український уряд не повинен шукати ілюзорних домовленостей з Путіним, а навпаки, збільшувати оборонну стратегію та можливості України та її інтеграцію до НАТО та Європейського Союзу. Але, насамперед, інтеграція до НАТО.

Таким чином, якщо ці три умови будуть дотримані, Крим і Донбас будуть повернуті, і Україна зможе розвиватися і стати процвітаючою країною. Якщо ці три прості умови не будуть дотримані, Україна не об'єднається ні з Кримом, ні з Донбасом, ставши або федеральним округом Росії, або окупованою територією.В цьому, власне, суть усієї Кримської платформи. Як на мене , Україна повинна більш пильніше ставитися до інформаційної безпеки .Потрібно вчасно висвітлювати проблеми, які відбуваються в країні, тоді б ми змогли уникнути анексію Криму , вберегти Донецьк і Донбас від ворожих намірів Росії. Адже люди би опиралися на чіткі факти , а не на пропаганду , яку пропонує наший ворожий сусід.

УДК 316.422
Семеній Д.М.
Котляров Д.П.
Національна академія Служби безпеки України

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

В наш час, коли ера інформаційних технологій та кібернетичного простору стрімко розвивається, люди, стають більш вразливими, ніж будь-коли раніше, а повсякденне життя кожного стає частиною кіберзлочинності. Сьогодні, одною з найбільш поширених атак є соціальна інженерія.

Соціальна інженерія - метод отримання необхідного доступу до інформації або виконання певних дій, заснований на особливостях психології людей. Основною метою соціальної інженерії є отримання доступу до конфіденційної інформації, паролів, банківських даних і інших захищених систем.

Зловмисники, намагаються використовувати людські слабкості, наприклад, квапливість, жадібність, альтруїзм чи страх перед офіційною установою з метою отримання конфіденційної інформації і подальшого доступу до систем(и).

Для того щоб забезпечити себе (ваших співробітників) від впливу соціальної інженерії, необхідне розуміння як вона працює.

Розглянемо основні типи соціальної інженерії та методи захисту від них:

- **Претекстінг** - це набір дій, відпрацьованих за певним, заздалегідь складеним сценарієм, в результаті якого жертва може видати будь-яку інформацію або вчинити певну дію [1].

- **Фішинг** - техніка інтернет-шахрайства, спрямована на отримання конфіденційної інформації користувачів - авторизаційних даних різних систем. Основним видом фішингових атак є підроблений лист, відправлений жертві по електронній пошті [1].

- **Троянський кінь** - це техніка ґрунтується на цікавості, страху або інших емоціях користувачів. Зловмисник відправляє жертві лист зі вкладенням, в якому знаходиться шкідлива програма для збору або зміни інформації. [1]

- **Кві про кво** (послуга за послугу) - дана техніка передбачає звернення зловмисника до користувача по електронній пошті або корпоративному телефону. Зловмисник може представитися, наприклад, співробітником технічної підтримки та інформувати про виникнення технічних проблем на робочому місці. Далі він повідомляє про необхідність їх усунення. У процесі «рішення» такої проблеми, зловмисник підштовхує жертву на вчинення дій, що дозволяють атакуючому виконати певні команди або встановити необхідне програмне забезпечення на комп'ютері жертви [1].

- **Зворотня соціальна інженерія** - даний вид атаки спрямований на створення такої ситуації, при якій жертва змушена буде сама звернеться до зловмисника за «допомогою» [1].

Основним способом захисту від методів соціальної інженерії є:

- проведення вступного та регулярного **навчання співробітників** компанії, спрямованого на підвищення знань з інформаційної безпеки. Всі працівники компанії мають бути попереджені про небезпеку розкриття персональної інформації та конфіденційної інформації компанії, а також про способи запобігання витоку даних. Крім того, у кожного співробітника компанії, в залежності від підрозділу і посади, повинні бути інструкції про те, як і на які теми можна спілкуватися зі співрозмовником, яку інформацію можна надавати для служби технічної підтримки, як і що повинен повідомити співробітник компанії для отримання тієї або іншої інформації від іншого співробітника.

- встановлене актуальне, **антивірусне програмне забезпечення.**

- виконання та дотримання **правил з інформаційної безпеки**:

- Призначені для користувача облікові дані є власністю компанії. Всім співробітникам в день прийому на роботу має бути роз'яснено те, що логін(и) і пароль(і), які їм видали, не можна використовувати в інших цілях (на web-сайтах, для особистої пошти тощо), передавати третім особам або іншим співробітникам компанії.
- Обов'язкова наявність регламентів з безпеки, а також інструкцій, до яких користувач повинен завжди мати доступ. В інструкціях повинні бути описані дії співробітників при виникненні тієї чи іншої ситуації (*приклад малюнок 1*).
- У корпоративній мережі компанії необхідно використовувати системи виявлення та запобігання атак.
- Необхідно максимально обмежити права користувача в системі (обмежити доступ до web-сайтам, заборонити використання знімних носіїв, тощо), але в рамках його функціональних обов'язків.

Виходячи з усього перерахованого, можна зробити висновок: основний спосіб захисту від соціальної інженерії - це навчання співробітників. Необхідно знати і пам’ятати, що незнання не звільняє від відповідальності. Кожен користувач системи повинен знати про небезпеку розкриття конфіденційної інформації і знати способи, які допоможуть запобігти витоку.

Малюнок 1.

Література

1. Зворотній соціальна інженерія. Техніки і терміни соціальної інженерії. Відомі соціальні інженери [Електронний ресурс]. – Режим доступу: https://beasthackerz.ru/uk/wi-fi-lokalnaya-set/obratnaya-socialnaya-inzheneriya-tehniki-i-terminy-socialnoi-inzhenerii.html.

УДК 631.95

Семенчук М.Р.
Національна академі Служби безпеки України

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ГІС ДЛЯ ЗАБЕЗПЕЧЕННЯ ВІЙСЬКОВИХ ТА МИРОТВОРЧИХ ОПЕРАЦІЙ У СВІТІ

Геоінформаційна система (далі - ГІС) за останнє десятиріччя став однією з найважливіших технологій для військової, миротворчої та іншої діяльності. Геопросторова інформація стала цінним доповненням для кращого розуміння місцевості, що є складовою військової майстерності та стратегічного управління загалом. Завдяки картам розповсюджувались знання про місцезнаходження об’єктів та було можливим інтерпретувати військові маневри противників. З часом, паперове картографування стало менш надійним та більш дорогим. У першу чергу, це пов’язано з тим, що

карти були надзвичайно дорогі товари для виготовлення. Точне картографування вимагає знання складної національної інфраструктури і потребує значного часу та зусиль для розробки та створення. Крім того, забезпечення доступності топографічного картографування у масштабі 1:50 000, яке вимагають військові командири, стало проблемою для оборонних картографічних організацій по всьому світу.

За досить невеликий проміжок часу ГІС здійснило революцію в командуванні та управлінні розстановкою військових сил та вдосконалило роботу військових установ, міжнародних організацій у проведенні миротворчих та інших місій.

Так, Картографічна секція ООН (UNCS) є основою геопросторових ініціатив Секретаріату ООН. Співробітники UNCS забезпечують географічну візуалізацію сесій Ради Безпеки, аналіз для Департаменту миротворчих операцій та Департаменту з політичних питань, а також картографічну підтримку звітів Генерального секретаря. UNCS також відповідає за програму ГІС для мирних операцій, керуючи офісами ГІС у 13 миротворчих та політичних місіях. Інші групи з управління інформацією, такі як співробітники ГІС та картографи в Управлінні з питань координації гуманітарних питань (OCHA), співпрацюють з UNCS для подальшого розширення сфери застосування ГІС.

У всіх органах ООН, що приймають рішення, покладаються на геоінформаційні продукти для підтримки високочутливих та важливих рішень, що залежать від геопросторових даних. Дані та аналіз ГІС використовуються для делімітації кордонів та демаркації, планування та операцій польових місій, гуманітарного втручання, логістики, розподілу ресурсів та критичного аналізу та візуалізації для поінформованості про певну ситуацію та можливі небезпеки [1].

Також, ця технологія широко використовується у роботі такої міжнародної міжурядової організації як військово-політичний блок НАТО. NATO Core GIS є основною геопросторовою інформаційною системою в рамках НАТО. Він надає НАТО широкий спектр послуг, зокрема геопросторові дані та геопросторові продукти. NATO Core GIS підтримує повний життєвий цикл геопросторової інформації, аби гарантувати, що всі етапи військових операцій проводяться з актуальної геопросторовою інформацією. Це стосується двох основних спільнот користувачів цієї системи: спеціалізованих геопросторових секцій та широкої спільноти користувачів функціональних служб. Ця система повністю заснована на COTS (готових комерційних продуктах), що використовує набір програмних продуктів ArcGIS від компанії Esri у конфігурації НАТО. Військові сили багатьох держав також використовують ГІС у різних сферах, включаючи картографію, розвідку, управління і аналіз стану поля бою, дослідження місцевості, дистанційне зондування, управління військовими об’єктами та моніторинг можливої терористичної діяльності [2].

Поява технології дистанційного зондування забезпечила оборонну силу необхідною інформацією. Супутники-шпигуни постійно отримують супутникові дані з високою роздільною здатністю в мирний час, щоб стежити за розробкою та придбанням сучасних пристосувань та потужностей ворожими силами для ведення війни. Що стосується цих супутників, то вони не дають конфіденційності, тому розвинені країни широко використовують методи дистанційного зондування для моніторингу діяльності із встановлення ядерних установок. Про них повідомляють також міжнародні агенції, що координують запобігання розповсюдження ядерній енергетиці в руйнівних цілях.

Використання даних дистанційного зондування у поєднанні з наземною інформацією забезпечує загальну платформу для аналізу наземних ситуацій під час війни. Включення супутників, що забезпечують зображення з високою роздільною здатністю, у сучасну епоху посилює здатність ГІС надавати більш точну та актуальну інформацію про військові операції.

Так, застосування новітніх технологій у картографії дозволяє вдосконалювати військовому сектору свої можливості, щоб зберегти надійний стримуючий фактор і дедалі ефективніше брати участь у миротворчих місіях. Саме тому ГІС відіграють ключову роль у створенні, редагуванні, аналізі, запитах та відображенні географічних даних, щоб допомогти командиру зрозуміти вплив місцевості на ведення бою. Проте, використання ГІС у військовій та оборонній сферах є обмеженим у зв’язку з технологічною неспроможністю деяких країн у забезпеченні широкого використання інформаційних технологій.

Література

1. UN Uses GIS to Promote Peace and Provide. URL: https://www.esri.com/news/arcnews/spring10articles/un-uses-gis.html (дата звернення: 07.03.2021 р.).

2. Military Applications of GIS. URL: https://www.geos.ed.ac.uk/~gisteac/gis_book_abridged/files/ch63.pdf (дата звернення: 07.03.2021 р.).

УДК 355.1

Толок Ю.С.
Державний університет телекомунікацій

ЗАГРОЗИ КРИТИЧНІЙ ІНФРАСТРУКТУРІ ТА ЇХ ВПЛИВ НА СТАН НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Відповідно до Стратегії національної безпеки України, загрозами безпеці критичної інфраструктури (КІ) визначено :

• критична зношеність основних фондів об’єктів інфраструктури України та недостатній рівень їх фізичного захисту;

• недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій;

• неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення.

Загрози КІ в разі їх реалізації проявлятимуться у вигляді припинення надання послуг та товарів, що є життєво важливими для населення, економіки, державного управління.

Серед основних загроз життєво важливим інтересам людини, суспільства, держави, які реалізуються за допомогою інформаційних, телекомунікаційних інформаційно-телекомунікаційних систем, є наступні:

– посягання на Інтернет-ресурси державних органів України з боку спецслужб інших держав, розвідувально-підривна діяльність іноземних/спеціальних служб з використанням кіберпростору;

– використання кіберпростору у військових цілях, розробка іноземними державами нових видів зброї кібернетичного характеру;

– зростаючі масштаби поширення кіберзлочинності;

– активізація проявів кібертероризму та інші.

Відзначається значне зростання інтенсивності кібератак, здійснюваних на інформаційно-телекомунікаційну інфраструктуру в Україні. Кібератак через мережу Інтернет зазнають сервери державних установ, великих компаній, фінансових установ, політичних партій та ЗМІ, інформаційно-телекомунікаційна інфраструктура воєнних об’єктів.

Джерелом загроз є не тільки незадовільний стан інфраструктурних мереж (їх висока зношеність, аварійність) та вплив природних факторів (карсти, зсуви, підтоплення та ін.), а ще і комплекс економічних факторів, що проявляються через незацікавленість операторів таких мереж поліпшувати ситуацію. В цілому це впливає на неефективне управління безпекою критичної інфраструктури, зокрема, систем життєзабезпечення. Так, суттєвою є загроза припинення надання життєво важливих послуг для населення через невирішені питання розрахунків між операторами інфраструктурних мереж та їх компаніями-постачальниками.

Незважаючи на визначення «комплексного вдосконалення правової основи захисту критичної інфраструктури» в Стратегії національної безпеки України в якості пріоритету забезпечення безпеки КІ, це завдання досі не покладено на жодний орган виконавчої влади.

Проблема відсутності чіткого визначення терміну «критична інфраструктура» в українському законодавстві, відповідно, відсутності переліку об’єктів такої категорії досі створює перешкоду для ефективного виконання невідкладних завдань забезпечення національної безпеки.

Завдання захисту КІ сфокусовані на попередженні кризових ситуацій, пов'язаних із функціонуванням такої інфраструктури. Без сумніву, моніторинг та прогнозування таких кризових ситуацій має здійснюватись із застосуванням сучасних інформаційних технологій та систем підтримки прийняття рішень, реалізованих у вузлах мережі ситуаційних центрів. При цьому має бути сформований координатор діяльності різних системи державного управління.

З метою узгодження діяльності різних систем державного управління доцільним є прийняття закону України «Про критичну інфраструктуру». В якому мають бути вказані принципи державної політики щодо захисту критичної інфраструктури, відображені питання державно-приватного партнерства в частині розподілу відповідальності, визначені повноваження органів державної влади із побудови системи захисту критичної інфраструктури, а також визначення термінів та зміни у пов'язані нормативно-правові акти.

Література

1. А.І. Семенченко, В.Л. Плескач, О.А. Заярний, М.В. Плескач / Наукова стаття / Організаційно-правові механізми державного управління забезпеченням кібербезпеки та кіберзахисту України: сутність, стан та перспективи розвитку / 2020 р.

2. Островий О. В. / Наукова стаття / Дослідження проблематики забезпечення кібернетичної безпеки в роботах українських науковців: джерельний аналіз / 2018 р.

3. Іванюта С. П. / Аналітична записка / Загрози критичній інфраструктурі та їх вплив на стан національної безпеки моніторинг реалізації Стратегії національної безпеки / 2017 р.

УДК 355.01

Уткін Г.А.
Національна академія Служби безпеки України

ГІБРИДНА ВІЙНА – ФОРМА СУЧАСНОГО КОНФЛІКТУ ДЕРЖАВ

В сучасному світі відбувається велика кількість різноманітних подій, які ми спостерігаємо кожного дня. Однією з найбільших та значущих для України подій – анексія Автономної Республіки Крим та здійснення агресії на території ОРДЛО.

З виникненням загрози територіальній цілісності та незалежності України загалом, українські науковці поринули у вивчення військових дій, тактики та стратегії агресії з боку Російської Федерації. Глибше дослідивши дане питання стало зрозуміло, що війна відбувається не в звичайному її прояві, не лише за допомогою зброї, але й з залученням засобів масової інформації, мережі Інтернет, соціальних мереж, та загалом вплив відбувається не

лише фізично, а й на свідомість та підсвідомість населення України. Зібравши достатньо інформації, було зроблено висновок, що війна сьогодні не звичайна, а є гібридною.

Головною відмінність сучасних конфліктів між державами є те, що вони використовують не лише традиційні методи, такі як: зброя, танки, кулемети та традиційний спосіб ведення війни, а й застосовують інформаційно – технічні, психологічні, соціальні, психічні інструменти. Завдяки розвитку технологій виникла змога використання більш розгорнутого переліку ресурсів, ніж це було раніше. Виникли соціальні мережі, Інтернет, розповсюдження інформації стало простіше, дешевше, а головне швидше.

Гібридну війну загалом розглядають як воєнні дії, які здійснюються шляхом поєднання традиційних та нетрадиційних методів ведення війни, які включають в себе інформаційний, економічний, психологічний, технічний вплив на противника задня досягнення поставлених цілей.

Організаційна структура «гібридної війни» має децентралізований вигляд, який приховує її реальну ієрархію. Зокрема, окремі ланки діють незалежно і намагаються виконувати свої завдання у відповідності до запропонованих загальних політичних цілей.

Таким чином, це позбавляє держави, які перебувають під «гібридним» нападом, оборонної стратегії, оскільки змінюються центри загрози; ці держави не в змозі визначити, де повинна бути встановлена лінія фронту і які інструменти слід використовувати для відбиття небезпеки.

Відсутність можливості оперативного виявлення чіткого зв’язку між гібридними засобами та їх організаційною ієрархічною структурою кардинально відрізняють «гібридну війну» від інших видів бойових дій [1].

Метою гібридної війни є створення дестабілізаційних процесів на території держави противника, руйнування критичної інфраструктури.

Етапи гібридної війни:

1 етап – підготовчий, під час якого вживаються заходи з формування ідеологічних, політичних та військових передумов майбутньої агресії.

2 етап – активні дії, а саме проведення прихованої агресії проти країни – противника з метою реалізації поставлених цілей та завдань.

3 етап – заключний, під час якого закріплюються позиції країни агресора на території країни – противника.

Висновки. Розвиток технологій створив нові можливості у веденні війни, виникла можливість застосування нових методів та способів проведення воєнного конфлікту. За допомогою ЗМІ, Інтернету, інформаційних ресурсів стало можливим застосовувати не лише звичайні методи впливу – зброю, танки, а й застосовувати інформаційні, психологічні, технічні ресурси.

Література

1. Війна «гібридна» // Політологічний енциклопедичний словник / уклад.: Л.М.Герасіна, В.Л.Погрібна, І.О.Поліщук та ін. / за ред. М. П. Требіна. – Харків: Право, 2015. – 816 с.

УДК 342.156
Фасоль О.О.
Національна академія Служби безпеки України

ПРІОРИТЕТИ РОЗВИТКУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ НА ПЕРІОД ДО 2030 РОКУ

Україна є суверенна і незалежна, демократична, соціальна, правова держава. Суверенітет України поширюється на всю її територію [1]. Історія її незалежності налічує не так багато років, всього близько 30-ти. З 2014 року в Україні тривають військові дії, розпочаті сусідньої країною-агресором, які направлені на знищення національної безпеки України, в тому числі на порушення її суверенітету та територіальної цілісності. З цього року і до сьогодні частина територій України перебуває у тимчасовій окупації країною-агресором.

Із вищевикладеного вбачається, що питання національної безпеки, створення та підтримання її системи є наразі дуже актуальним. При безвідповідальному чи несистемному ставленні до цього питання Україна, як незалежна країна, може припинити своє існування. Саме вбачаючи актуальність цієї проблеми, Президентом України наприкінці 2020 року було затверджено «Стратегію національної безпеки України».

П. 1.9 ст. 1 ЗУ «Про національну безпеку України» визначено, що «національна безпека України - захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз». В тому ж законі п.1.10 визначено, що «національні інтереси України - життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян» [3]. Тобто пріоритети розвитку системи національної безпеки повинні бути направленні на забезпечення безпеки держави, державного ладу, людини та її добробуту з урахуванням можливих загроз.

Розглянемо надважливий документ, а саме «Стратегію національної безпеки України» (далі – Стратегія), затверджену 14 вересня 2020 року указом Президента України № 392/2020 [2]. Стратегія визначає актуальні загрози національній безпеці України та відповідні цілі, завдання, механізми захисту національних інтересів України та є основою для планування і реалізації державної політики у сфері національної безпеки. Основним пріоритетом розвитку національної безпеки України вказано безпеку людини, яка безпосередньо впливає на безпеку країни. П.1 Стратегії говорить про те, що «Людина, її життя і здоров'я, честь і гідність, недоторканність і без-

пека – найвища соціальна цінність в Україні» [2]. В п. 2 та 3 Стратегії вказано, що «Україна прагне миру. Мир – запорука розвитку України. Встановлення миру, відновлення суверенітету і територіальної цілісності України у межах її міжнародно визнаного державного кордону – найвищий пріоритет держави» [2].

Отже, пріоритетами розвитку національної безпеки України до 2030 року, враховуючи ситуацію зумовлену військовими діями, буде безпека людини, безпека держави та мир.

Крім того, на думку автора, в Стратегії національної безпеки України недостатньо уваги приділено екологічній безпеці. На даний час військові, загарбницькі дії можуть розгортатися не тільки, як збройний конфлікт, а і через більш тривалі, приховані дії, наприклад, через екологічний геноцид українського народу. В свою чергу 28.02.2018 р. ЗУ № 2697-VIII були затверджені основні засади (стратегія) державної екологічної політики України на період до 2030 року [4]. Цей документ направлений на охорону надр, вод, біологічної безпеки, екологічної безпеки Донбасу тощо.

Особливістю України є те, що джерелом загроз незалежності, її суверенітету і демократії залишається недостатня ефективність державних органів та корупція, законотворці у гонитві за кількістю законодавчих ініціатив та підняттям свого особистого рейтингу, втрачають послідовний, практичний та конкретний зміст документів. Постійні реформи, що не доводяться до кінцевого результату протидіють ефективному управлінню ресурсами та їх розподілу. На тлі зростання викликів і посилення загроз національній безпеці зберігається невідповідність сектору безпеки і оборони України завданням захисту національних інтересів.

Отже, враховуючи вищевикладене, можна зробити висновки, що з існуючих законодавчих документів в цілому зрозумілі пріоритети розвитку національної безпеки України на період до 2030 року, але для ефективної їх реалізації необхідний ряд підзаконних нормативно-правових актів, із чітким визначенням тактичних завдань кожної сфери національної безпеки та суб’єктів їх виконання. Крім того, на думку автора, необхідно розширити потенційні загрози національній безпеці в Стратегії національної безпеки шляхом визначення всіх можливих чинників впливу на сфери життя людини, суспільства та держави, а не виключно країни-агресора на сьогоднішній день.

Література

1. Конституція України [Електронний ресурс] // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – с. 141. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

2. Указ Президента «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України"» [Електронний ресурс] // – Режим доступу : https://zakon.rada.gov.ua/laws/show/392/2020#Text.

3. Закон України «Про національну безпеку України» [Електронний ресурс] // Відомості Верховної Ради (ВВР). – 2018. – № 31. – с.241. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469-19#Text.

4. Закон України «Про основні засади (стратегія) державної екологічної політики України на період до 2030 року» [Електронний ресурс] // Відомості Верховної Ради (ВВР). – 2019. – № 16. – с. 70 – Режим доступу : https://zakon.rada.gov.ua/laws/show/2697-19#Text.

УДК 004.7

Федоров І.А.
Харківський національний університет радіоелектроніки

ПРОГРАМНО АПАРАТНИЙ СИМУЛЯТОР ІНФРАСТРУКТУРИ КОМПАНІЙ

Сьогодні організації направляють все більше коштів на впровадження новітніх технологій у рамках проектів цифрової трансформації, яке не тільки створює багато нових можливостей, але й приводить до появи нових вразливостей та загроз. При цьому необхідно розуміти, що без довіри зі сторони користувача така трансформація не може бути успішною. Кібербезпека повинна стати частиною корпоративної філософії, а для цього, як мінімум, її слідує інтегрувати в стратегію розвитку бізнесу [1].

Стратегія кібербезпеки України передбачає розвиток кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, кіберзахист критичної інфраструктури, розвиток потенціалу сектору безпеки та оборони у сфері забезпечення кібербезпеки, боротьбу з кіберзлочинцями.

В розвиток визначених задач є актуальним підготовка кваліфікованих фахівців з кібербезпеки. Для досягнення цієї мети пропонується створення програмно-апаратного комплексу для моделювання систем різного функціонального призначення, налаштованого під задані, певні операційні системи та конфігурації. Призначення цього комплексу є створення тренажеру для моделювання та оцінки захищеності об’єктів кіберзахисту: комунікаційних систем, які використовуються у сфері електронного управління, електронних державних послуг, електронної комерції, електронного документообороту.

Запропонований програмно-апаратний комплекс побудовано на мікрокомп’ютерах Raspberry Pi 4 та orange Pi One, роутеру Mikrotik та свічу Mikrotik. Структурна схема комплексу представлена на рис 1. Для моделювання вразливих ОС були розроблені власні, спеціально вразливі, дистрибутиви на базі операційної системи Linux, на них додатково розміщується сайт, сервер та інші застосування.

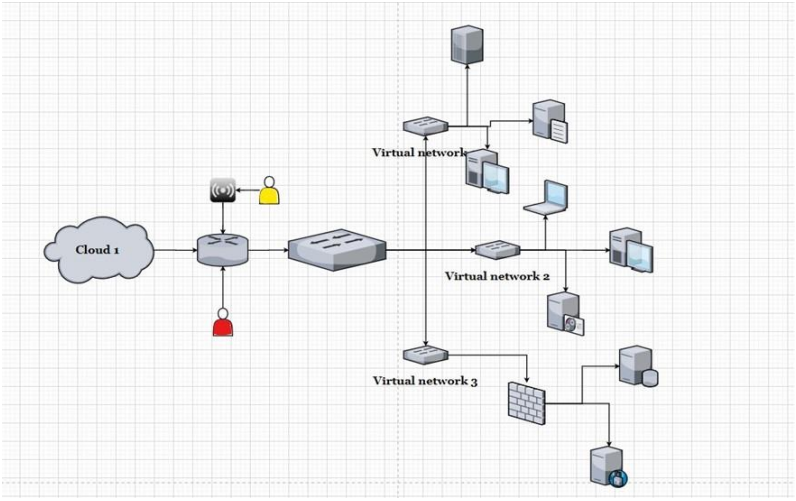


Рис. 1. Загальна схема комплексу

Вибір запропонованої схеми визначається простотою використання, функціональною повнотою та достатньо низькою вартістю.

Функціонал програмно-апаратного комплексу дозволяє:

– моделювати сучасні системи та відпрацьовувати атаки с використанням їх вразливостей;
– відстежувати інциденти в інформаційних системах;
– виявляти підозрілий трафік у мережі;
– здійснювати побудову захищених систем;
– моделювати кіберзлочіни, та організовувати процес їх розслідування.

На даний час на базі даного комплексу можна відпрацювати декілька вразливостей, найрозповсюджених в інформаційному просторі [2]:

– тестування баз даних за допомогою SQL ін’єкцій;
– використання вразливості у PHP сервері (запуск шкідливого коду в картинці);
– використання вразливість у плагені сайту, який міняє мову сайту, та подальша його експлуатація для отримання прав root;
– використання вразливості Eternal Blue;
– використання вразливості FTP;
– пошук паролів для SSH з’єднання та отримання прав root.

Таким чином, завдяки використанню цього комплексу можливий відхід від віртуалізації в навчанні та перехід до побудови реальних систем з можливістю побудови та перевірки систем їх захисту.

Література

1. Brill, Alan, Kristina Misheva, and Metodi Hadji-Janev, eds. Toward Effective Cyber Defense in Accordance with the Rules of Law. Vol. 149. IOS Press, 2020.

2. Richard Stiennon. Cyber Defense: Countering Targeted Attacks. Rowman & Littlefield Pub Incorporated, 2012. – 192 с.

УДК 329.09.5(477)
Холдоєнко А.В.
Харківський національний університет внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА В КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Сьогодення являє собою насичений, динамічний простір, який кожного дня піддається глобальному розвитку і створенню чогось новітнього. Людство ввійшло в епоху інформаційного суспільства, де саме інформація є провідним чинником в більшості сфер життєдіяльності. Право, політика, економіка, освіта, медицина, релігія, культура, оборона, сфери послуг дозвілля і розваг – усі ці сфери на сьогоднішній момент неможливо уявити без впливу інформаційних технологій.

Людина завжди «приречена» на пошук, оцінку та захист інформації (різниця полягає тільки за змістом – інформація про місця для полювання, джерело води, інше плем'я чи щодо комерційної таємниці і персональних даних), тобто, інформаційну діяльність, яка нерозривно пов'язана з інформаційною безпекою. Тільки от за умови формування інформаційного суспільства значення останньої невпинно зростає [1, с. 129].

Інформація – це важіль сили і влади, і в різних ситуаціях вона може мати різносторонні наслідки, як приклад, у одержувачів інформації можуть виникнути сумнівів, або навіть перетворитися у зброю, яка може нести руйнівні наслідки як для кожної особи, так і для суспільства в цілому.

Проте, оперуючи інформацією, потрібно бути переконаним у тому, що використовувана інформація якісна й у процесі передачі, поширення не була спотворена. Тому питання інформаційної безпеки є важливим компонентом усієї системи національної безпеки країни [2, с. 65].

Законодавча дефініція інформаційної безпеки міститься в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.»: «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [3].

У цій дефініції сутність інформаційної безпеки розкривається через визначення певних ключових елементів (об'єктів) цього явища, щодо яких потрібно вжити заходів забезпечення безпеки з метою унеможливлення шкоди. Такими елементами є:

– якість інформації, котру використовують (забезпечення її повноти, вчасності та вірогідності);

– правила інформаційної діяльності (запобігання негативному інформаційному впливу та негативним наслідкам застосування інформаційних технологій);

– правові режими інформаційних ресурсів та доступу до інформації (забезпечення виконання визначених законодавством правил розповсюдження та використання інформації, а також її цілісності, конфіденційності та доступності інформації) [4, с.130].

З приводу інформаційної безпеки важливою є думка О.А. Баранова, який деталізує виклики і загрози при визначенні інформаційної безпеки як стану захищеності життєво важливих інтересів особистості, суспільства і держави, за якого зводиться до мінімуму заподіяння збитків через неповноту, несвоєчасність і недостовірність інформації, через негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [5, с.160]

Зрозуміло, що сьогодні українське суспільство перебуває під постійною загрозою отримання недостовірної, а подеколи – шкідливої інформації, її несвоєчасного надходження, шпигунства, комп'ютерної злочинності тощо. Ці фактори є елементами гібридної війни, які сприяють вторгненню агресора в національну свідомість громадян, підриву національної та інформаційної безпеки. Пріоритетами державної політики в інформаційній сфері мають бути: забезпечення інформаційної безпеки, забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію, відкритість та прозорість держави перед громадянами, формування позитивного міжнародного іміджу України [6].

Політика інформаційної безпеки має комплексний характер та включає внутрішньо- та зовнішньополітичні, економічні, оборонні, технологічні складові. Отже, інформаційна безпека - це стан захищеності життєво важливих інтересів людини, суспільства і держави, який є складовою загальної системи національної безпеки, включаючи в себе діяльність органів державної влади, котрі повинні злагоджено здійснювати свою роботу на основі правових норм, які є єдиними для всіх на території держави, задля ефективного протистояння загрозам в інформаційній сфері в сучасних умовах.

Література

1. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. – Київ :ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.

2. Задірака В.К. Сучасні методи розв'язання задач інформаційної безпеки. Вісник НАН України. 2014. № 5. С. 65–69.

3. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр. : Закон України від 09 січня 2007 р. № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text.

4. Кормич Б. А. Інформаційне право. Підручник. – Харків: БУРУН і К., 2011. – 334 с.
5. Баранов О.А. Інформаційна безпека і економічні перетворення. Поглиблення ринкових реформ та стратегія економічного розвитку України до 2010 року: Мат. міжнародної конференції. К., 1999. Ч. 2, т. 1. 168 с.
6. Доктрина інформаційної безпеки України. Указ Президента України від 27 лютого 2017 р. № 47/2017 URL: https://zakon.rada.gov.ua/laws/show/47/2017#n12/.

УДК 004.056.5
Шилов М.С.
Жевелєва І.С.
кандидат юридичних наук,
Національна академія Служби безпеки України

УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ОРГАНІЗАЦІЯХ

Всі організації, установи, підприємства, що керуються сучасними технологіями, зобов'язані вживати заходи захисту інформаційної безпеки, якщо вони зацікавлені успішному, а головне безпечному майбутньому своєї компанії. Сучасні технології здатні протидіяти кібернетичним атакам, але цього не достатньо, організації повинні забезпечити, щоб виробничі процеси, політика та поведінка працівників сприяла мінімізації і протидії ризикам. Для забезпечення захисту ІБ потрібно діяти системно. На допомогу сучасним підприємствам приходять системи управління інформаційною безпекою.

Система управління інформаційною безпекою (СУІБ) - це структура політик та засобів контролю, які систематично керують безпекою та ризиками на всьому вашому підприємстві. Ці засоби контролю безпеки можуть відповідати загальним стандартам безпеки або бути більш зосередженими на вашій галузі. Наприклад, ISO 27001 - це набір специфікацій, що детально описують, як створювати, керувати та впроваджувати політики та засоби управління СУІБ. ISO не передбачає конкретних дій, натомість він надає настанови щодо розробки відповідних стратегій системи управління інформаційною безпекою [1].

Проведення комплексу заходів із побудови системи управління інформаційною безпекою відповідно до вимог стандарту ISO 27001 дозволить вирішити такі завдання: підвищення рівня безпеки. Стандарт розроблений з урахуванням кращих світових практик забезпечення інформаційної безпеки; управління. Стандарт передбачає побудову циклічного і керованого процесу забезпечення інформаційної безпеки; Оптимізація витрат. СУІБ дозволяє оптимізувати і обгрунтувати витрати на інформаційну безпеку; ризики. Зниження рівня фінансових ризиків, пов'язаних з інформаційною

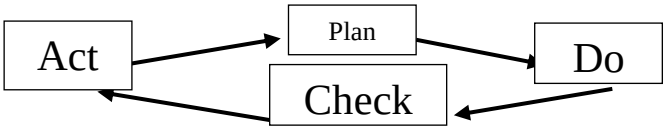
безпекою, шляхом їх ідентифікації, оцінки та прийняття адекватних захисних заходів; привабливість. Підвищення ступеня привабливості компанії на внутрішньому і зовнішньому ринках (конкурентні переваги; довіра. Підвищення довіри з боку акціонерів, клієнтів, партнерів і контрагентів; репутація. Підвищення рівня ділової репутації шляхом сертифікації СУІБ, яка демонструє високий рівень зрілості компанії [2].

Основи системи управління інформаційної безпеки зазвичай зосереджені на оцінці ризиків та управлінні ними. Організації, що працюють у жорстко регульованих галузевих вертикалях, таких як охорона здоров'я або національна оборона, можуть вимагати широкого кола заходів безпеки та стратегії зменшення ризику, тобто постійного вдосконалення інформаційної безпеки.

Хоча система управління інформаційною безпекою призначена для створення цілісних можливостей управління інформаційною безпекою, цифрова трансформація вимагає від організацій постійного вдосконалення та вдосконалення своїх засобів безпеки. Структура та межі, визначені СУІБ, можуть застосовуватися лише протягом обмеженого періоду часу, і робоча сила може боротися з їх прийняттям на початкових етапах. Завданням організацій є еволюція цих механізмів контролю безпеки, оскільки їх ризики, культура та ресурси змінюються.

Відповідно до ISO 27001, впровадження СУІБ дотримується моделі Plan-Do-Check-Act (PCDA) для постійного вдосконалення процесів (мал. 1):

- Плануйте (Plan). Визначення проблеми та збирання корисної інформації для оцінки ризику безпеки. Знаходження політики та процесів, які можна використовувати для усунення першочергових проблем.
- Робіть (Do). Впровадити розроблену політику та процедуру безпеки.
- Перевірте (Check). Моніторинг ефективності політики та засобів управління системою управління інформаційною безпекою.
- Дійте (Act). Зосередьтеся на постійному вдосконаленні. Документуйте результати, діліться знаннями та використовуйте цикл зворотного зв'язку [3].



Мал. 1. Модель постійного вдосконалення процесів

Отже, система управління інформаційною безпекою і сертифікація на відповідність стандарту ISO 27001 дає компанії такі переваги:

управління інформаційною безпекою компанії в рамках єдиної корпоративної політики, управління ризиками та їх своєчасне виявлення, зниження ризиків від зовнішніх і внутрішніх загроз, систематизація процесів забезпечення ІБ, встановлення пріоритетів компанії в області ІБ. У свою

чергу це забезпечує організації конкурентну перевагу, демонструючи здатність керувати інформаційними ризиками, при цьому також збільшується довіра компанії.

Література

1. https://www.turcert.com/uk/belgelendirme/sistem-belgelendirme/iso-27001-bilgi-guvenligi-yonetim-sistemi.

2. Побудова системи управління інформаційною безпекою // [Електронний ресурс]. – Режим доступу: – http://unit.com.ua/ua/postroenie-sistemy-upravleniya.

3. Система управління інформаційною безпекою // [Електронний ресурс]. – Режим доступу: – https://core.ac.uk/download/pdf/48401951.pdf.

УДК 341.123(045)(0.034.2PDF)

Шнайдерський І.С.
Національна академія Служби безпеки України

ОКРЕМІ ПИТАННЯ ПРАВОВОГО СТАТУСУ ПРЕЗИДЕНТА УКРАЇНИ ІЗ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

У приписах статті 17 Конституції України визначено, що захист суверенітету та територіальної цілісності України є однією з найважливіших функцій держави. Її виконання потребує реформування та розвитку сектору безпеки і оборони, підвищення його спроможності адекватно і гнучко реагувати на загрози державній безпеці України. Це досягається, зокрема, шляхом реалізацією повноважень Президента України у сфері національної безпеки у співвідношенні з його загальним правовим статусом.

На сьогодні численні публікації, присвячені правовому статусу Президента України насамперед із точки зору конституційного права (праці Ю. Барабаша, Д. Бєлова, Ф. Бурчака, О. Даниляка, А. Кудряченка, В. Скрипнюка, О. Спіріна, В. Сухоноса, Ю. Тодики, А. Яковлєва та багатьох інших). Окремі роботи, що стосуються обсягу повноважень Президента України та напрямів їх реалізації у сфері національної безпеки і оборони (роботи Ю. Михайлової, П. Рудика, В. Сазонова та ін.), опосередковано торкаються контрольного складника зазначених повноважень. Тому не втрачає актуальності окремі питання правового статусу Президента України із забезпечення національної безпеки і оборони України.

Враховуючи зазначене, Президенту України як Верховному Головнокомандувачу Збройними Силами України та гаранту державного суверенітету і територіальної цілісності України й повинна бути підпорядкована вся сфера державного управління обороною та забезпеченням національної безпеки країни.

У сфері національної безпеки й оборони Президент України здійснює політичне керівництво органами, які забезпечують національну безпеку й обороноздатність України.

Зокрема, Раду національної безпеки і оборони України (далі – РНБО) – координаційний орган із питань національної безпеки й оборони – очолює Президент України. Головування в РНБО зумовлено тим, що принцип єдиноначалля в керівництві обороною і централізоване управління вимагають від Президента не загального, а конкретного керівництва системою органів, які забезпечують безпеку й оборону держави. Відповідно до ч. 2 ст. 107 Конституції України, функціями РНБО є координація та контроль за діяльністю органів виконавчої влади у сфері національної безпеки й оборони. Це один із допоміжних органів при Президентові України, який забезпечує реалізацію його відповідних повноважень у сфері діяльності органів виконавчої влади. Правовий статус цього органу та компетенція - похідні від владних повноважень Глави держави. Діяльність Ради національної безпеки і оборони України й головування Президента України в цьому органі відіграють суттєву роль у поєднанні функцій Глави держави з виконавчою владою.

Відповідно до п. 12 ст. 85 Конституції України, Верховна Рада України призначає Прем'єр-міністра України, Міністра оборони України та Міністра закордонних справ України за поданням Президента України. Виходячи з цього Президент України має вплив на діяльність Кабінету Міністрів України у сфері національної безпеки й оборони засвідчує і порядок призначення Прем'єр-міністра України, а також порядок призначення і звільнення Міністра оборони України та Міністра закордонних справ України.

Верховна Рада України припиняє повноваження як Кабінету Міністрів України загалом (ст. 87 Конституції України), так і окремих міністрів (п. 12 ст. 85 Конституції України). Відповідно до Закону України "Про Кабінет Міністрів України" від 27 лютого 2014 р., Верховна Рада України має право звільняти міністрів Кабінету Міністрів України як самостійно, так і за поданням Прем'єр-міністра України (ч. 1 ст. 18). При цьому стосовно Міністра оборони України та Міністра закордонних справ України таке подання вноситься за згодою Президента України. Звільнення з посади Міністра оборони України та Міністра закордонних справ України можливе також за ініціативою Президента України шляхом його відповідного подання до Верховної Ради України. Очевидно, що порядок призначення та звільнення цих міністрів враховує їх особливу роль у реалізації повноважень Президента України у сфері національної безпеки й оборони.

Відповідно до п. 7 ст. 116 Конституції України, здійснення заходів щодо забезпечення національної безпеки й оборони є власним повноваженням Кабінету Міністрів України. Це означає, що координація діяльності органів виконавчої влади у сфері національної безпеки й оборони, яку здійснює Президент України, не обмежує відповідної компетенції Кабінету Мі-

ністрів України. Отже, забезпечення національної безпеки й оборони належить до сфери сумісної компетенції Глави держави й Уряду. Тому реалізація функції Президента України із забезпечення національної безпеки й оборони безпосередньо пов'язана з діяльністю в цій сфері Кабінету Міністрів України.

Відповідно до п. 121 ст. 85 Конституції України, до компетенції Верховної Ради України належить "призначення на посаду та звільнення з посади за поданням Президента України Голови Служби безпеки України". Водночас, відповідно до п. 1 ст. 106 Основного Закону України, державну незалежність і національну безпеку забезпечує Президент України [1].

Також важливим вбачається, що в умовах проведення реформи децентралізації в Україні, Президент України Володимир Зеленський під час засідання Ради розвитку громад та територій у межах Всеукраїнського форуму «Україна 30» наголосив, що «…децентралізація реально втілюється у життя, а також рівень життя, безпеки, здоров'я, освіти, комфорту й добробуту українців залежить від рівня взаємодії між органами влади» [2].

Таким чином, в умовах реформування окремих суспільних сфер життя (земельна, медична, освітня, судова, конституційна, реформа децентралізації), а також у змінах до Конституції України необхідно, зокрема передбачити норми щодо гарантування матеріальної та фінансової основи місцевого самоврядування, але разом з тим необхідно передбачити низку запобіжників, щоб з децентралізацією не відбулося послаблення повноважень Президента України та центральної влади в таких питаннях, як оборона, зовнішня політика, національна безпека, верховенство права, дотримання прав і свобод людини і громадянина України.

Література

1. Конституція України [Електронний ресурс] // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – С. 141.

2. Президент обговорив з народними депутатами питання реформи децентралізації [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua.news/president-obgovoriv.

УДК 004.056

Юрчак І.І.
Національна академія Служби безпеки України

УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Питання управління інцидентами інформаційної безпеки з кожним днем все гостріше постає перед сучасним суспільством, адже технології безупинно розвиваються, створюються нові, вдосконалюються вже існуючі.

Інформація стала найціннішим ресурсом сьогодення, саме тому, створюються і потенційні або реальні загрози інформації та інформаційній безпеці в цілому. Розглянемо поняття інформаційної безпеки глибше.

Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення [1].

При створенні загрози – подія, яка не є елементом нормального функціонування, потрібно застосовувати управління інцидентами, яка являється однією з найважливіших процедур управління інформаційною безпекою.

Під поняттям «інцидент» розуміється подія, що не є елементом нормального та правильного функціонування сервісу і при цьому створює, або здатна створити загрозу функціонування сервісу шляхом його переривання або зниження якості.

Відповідно до чинних міжнародних нормативно – правових актів управління інцидентами інформаційної безпеки існує регламент дій, яких потрібно притримуватись. Першим кроком є своєчасне та швидке усунення наслідків інциденту, для мінімізації збитків.

Наступним кроком є розслідування інциденту, виконати оцінку необхідності дій щодо усунення причини інциденту та за необхідності реалізувати їх, а також застосувати превентивні заходи при повторному виникненні інциденту в майбутньому.

Управління інцидентами інформаційної безпеки регламентуються такими нормативно – правовими актами:

- ISO 20000
- ISO/IEC 27001
- ISO/IEC 27035
- CMU/SEI-2004-TR-015
- NIST SP 800-16
- ITU-T X-1051
- ITU-T E.409

В більшості випадків, якщо у суб’єкта відсутні інциденти, це лише означає відсутність їх фіксації. Інцидент може відбуватись в даний момент, а можливо відбудеться в майбутньому, саме тому необхідно приділяти увагу інформаційній безпеці та управлінню інцидентами.

Розробка і реалізація процесу управління інцидентами ІБ відповідно до кращих практик забезпечує чітке визначення ролей і відповідальності всіх фахівців за якісне і своєчасне реагування на інциденти ІБ; надавати опера-

тивну інформацію для моніторингу ефективності прийнятих захисних заходів; надавати необхідну інформацію для коректного проведення аналізу ризиків ІБ [2].

Отже, ми розглянули питання інформаційної безпеки та глибше дослідили управління інцидентами інформаційної безпеки, розглянули порядок дій при виникненні інциденту та зазначили важливість виконання вищезазначених дій.

Література

1. Коваленко, Ю. О. (2010). Забезпечення інформаційної безпеки на підприємстві. Економіка промисловості (3). с. 123–129. Процитовано 2019-11-16.

2. Розслідування інцидентів інформаційної безпеки // [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/bitstream/123456789/9600/1/11.pdf.

РЕКОМЕНДАЦІЇ
науково-практичної конференції
«Актуальні проблеми управління інформаційною безпекою держави»

26 березня 2021 року Національною академію СБ України спільно з Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Інститутом модернізації змісту освіти Міністерства освіти і науки України проведено XII Всеукраїнську науково-практичну конференцію ***«Актуальні проблеми управління інформаційною безпекою держави».***

Зважаючи на складну епідеміологічну ситуацію конференція відбулася в заочній формі. До організаційного комітету конференції подали тези доповідей представники Апарату Ради національної безпеки і оборони України, Міністерства цифрової трансформації України, Міністерства оборони України, Міністерства внутрішніх справ України, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, Національної ради України з питань телебачення і радіомовлення тощо, а також понад **25** провідних наукових установ і закладів вищої освіти України.

Роботу конференції було присвячено розгляду актуальних проблем забезпечення інформаційної та кібернетичної безпеки, зокрема, питань негативного інформаційного впливу на шкоду людини, суспільства і держави, протидії кібертероризму та кіберзлочинності, захисту кібербезпеки об'єктів критичної інфраструктури України.

За результатами обговорення вказаних та інших питань учасники конференції ***к о н с т а т у в а л и*:**

1) сучасні світові процеси глобалізації та цифрової трансформації уможливили поширення міжнародного інформаційного тероризму й міжнародної кіберзлочинності. Виникли нові загрози національній та міжнародній безпеці, які носять інформаційний характер та здатні завдати значної шкоди інтересам людини, суспільства і держави;

2) гібридна війна Російської Федерації проти України, що здійснюється з використанням новітніх технологій інформаційного впливу на свідомість громадян та інформаційну інфраструктуру, спрямована на підрив національної безпеки та обороноздатності держави, розпалювання міжнаціональних та міжрелігійних конфліктів, провокування масових заворушень та зміни конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності України та загострення суспільно-політичної ситуації в Україні;

3) комплексний характер реальних та прогнозованих загроз національним інтересам і національній безпеці України в інформаційній сфері потребує формування та реалізації ефективної державної інформаційної політики, дієвої координації та взаємодії сил безпеки і оборони в інтересах захисту і розвитку національного інформаційного простору, запобігання його можливого використання на шкоду національним інтересам України та протидії інформаційній агресії.

Учасники конференції рекомендують:

1) долучитися вченим та експертам сектору безпеки і оборони до опрацювання Стратегії інформаційної безпеки України, що розробляється робочою групою Міністерства культури та інформаційної політики України, а також до підготовки пропозицій щодо розвитку засад державної інформаційної політики України;

2) продовжити наукові дослідження і розробки та впровадження новітніх технологій і методів пошуку, виявлення, оцінки, запобігання та припинення реальних і потенційних загроз у сфері інформаційної та кібернетичної безпеки України, передусім щодо механізмів негативного інформаційного впливу на шкоду життю і здоров'ю людини, інформаційних посягань на життєво важливі інтереси суспільства і держави та кіберзахисту об'єктів критичної інфраструктури;

3) забезпечити активне залучення наукового та експертного середовища до імплементації стандартів Європейського Союзу з питань захисту даних, а також стандартів забезпечення кібербезпеки країн-членів НАТО у законодавство України;

4) забезпечити подальший розвиток системи забезпечення інформаційного суверенітету, управління ризиками та новітніми можливостями в інформаційній сфері та кіберсфері, розбудову інформаційно-комунікаційної інфраструктури, формування національного інформаційного простору, оптимізації взаємодії та комунікаційного процесу між державними органами, органами місцевого самоврядування та споживачами інформаційної продукції і послуг;

5) вжити необхідних заходів щодо становлення і розвитку системи стратегічних комунікацій сектору безпеки і оборони, як скоординованого і належного використання комунікативних можливостей публічної дипломатії, зв'язків з громадськістю, військових зв'язків, інформаційних та психологічних операцій, а також інших заходів, спрямованих на просування цілей держави;

6) удосконалити комплекс інформаційних та організаційно-правових заходів щодо формування позитивного іміджу України у світі, донесення оперативної, достовірної й об'єктивної інформації про події в країні до міжнародної спільноти та своїх громадян;

7) організувати цільові наукові дослідження і розробки, спрямовані на розбудову систем забезпечення інформаційної та кібернетичної безпеки України з урахуванням пріоритетних напрямів правових досліджень з питань *«Правового забезпечення інформаційної сфери», «Правового забезпечення у сфері цифрової трансформації»* і *«Правового забезпечення у сфері національної безпеки та оборони»,* визначених Стратегією розвитку Національної академії правових наук України на 2021-2025 роки, яка координує правові дослідження відповідно до законодавства;

8) забезпечити активне залучати до наукових досліджень з проблем управління інформаційною безпекою держави молодих учених, курсантів та студентів;

9) сприяти в контексті європейської та розвитку міжнародного співробітництва з питань забезпечення інформаційної безпеки та кібербезпеки.

ЗМІСТ

Вступне слово 3

ПРІОРИТЕТИ РОЗВИТКУ СИСТЕМИ ІНФОРМАЦІЙНОЇ І НАЦІОНАЛЬНОЇ БЕЗПЕКИ НА ПЕРІОД ДО 2030 РОКУ

Антипенко І.В. Перспективні напрями впровадження національної оцінки політичних ризиків в Україні 5

Арсенович Л.А. Шляхи формування системи підготовки кадрів у сфері кібербезпеки органів державної влади України в умовах розвитку цифрового суспільства України 7

Богуцький П.П. Санкції у системі правового забезпечення національної безпеки України в інформаційній сфері 9

Богуш В.М., Бровко В.Д., Мамченко С.М. Підготовка фахівців з кібербезпеки в межах спеціальності 256 національна безпека (забезпечення національної безпеки в інформаційній сфері та кіберпросторі)..... 12

Ватраль А.В. Демократичний цивільний контроль за діяльністю спеціальних служб у контексті розвитку системи забезпечення національної безпеки України..... 15

Вдовенко С.Г., Даник Ю.Г. особливості забезпечення раціонального розвитку кібербезпеки і кібероборони держави 17

Войтко О.В., Солонніков В.Г. Державна інформаційна політика основа забезпечення інформаційної безпеки в умовах гібридної війни 19

Горовий В.М. Національні стратегічні комунікації у взаємодії з глобальним інформаційним простором..... 22

Гребенюк А.В. Антиукраїнська пропаганда: актуальні проблеми визначення поняття та риси 24

Грига М.А. Окремі особливості огляду електронних документів..... 27

Давиденко М.О. Напрями протидії поширенню релігійного екстремізму в інформаційному середовищі в умовах гібридної війни 29

Даник Ю.Г. Особливості раціонального розвитку системи підготовки фахівців і наукових досліджень з високотехнологічних оборонних напрямів для сектору безпеки і оборони України, включаючи інформаційну та кібербезпеку 31

Даниленко В.М. Загрози для національної безпеки України у науково-освітньому дискурсі РФ 33

Дзьобань О.П. Концептуалізація поняття «мережева війна» у проблемному полі вітчизняного безпекознавства 36

Іванов О.Ю. З історії російсько-польського інформаційного протиборства: досвід для України 38

Іванова В.М. Зовнішньоекономічна безпека: огляд наукових підходів 41

Князєв С.О. Упорядкування законодавчого визначення терміна «охорона державної таємниці» 43

Клименко О.М., Какауліна Л.М. До питання правового забезпечення напрямків державної політики у сфері національної безпеки 45

Коваленко Є.В., Плетньов О.В. Інформаційна інфраструктура держави як об’єкт забезпечення кібернетичної безпеки 48

Козубцов І.М., Козубцова Л.М. Прогноз можливих наслідків настання «колапсу інформаційних систем спеціального призначення» 50

Козюра В.Д., Хорошко В.О. Проблеми управління уразливостями в інформаційно-телекомунікаційних системах 53

Комаров В.С., Олексіюк В.В., Балик І.В. Удосконалення розвідувальної діяльності як складової системи забезпечення національної безпеки держави 56

Корж І.Ф. Проблеми інформаційної безпеки України в сучасних умовах 58

Куцій М.С. Вразливість системи як проблема реалізації відкритої архітектури на об’єктах технічного захисту інформації 60

Ланде Д.В., Дмитренко О.О. Побудова онтологічних моделей у галузі права 62

Лаптєв О.А., Гребенніков А.Б., Лаптєв С.О., Загиней А.Ю. Модель захисту інформації при нелінійних параметрах зовнішніх впливів з урахуванням взаємодії користувачів 64

Мацик Ю.Й. Розвиток інтернету та кібергігієна 66

Мельник Д.С. Щодо сучасних загроз національній безпеці України в інформаційній сфері 68

Міхєєв Ю.І. Шляхи удосконалення інформаційно-аналітичного забезпечення збройних сил України в національному сегменті кіберпростору 71

Огарок А.П. Підхід до створення системи забезпечення інформаційної безпеки розвідувальних органів України 73

Олєйніков Д.О. Щодо необхідності кримінально-правової охорони інформаційної безпеки держави 75

Онищенко Ю.М., Світличний В.А. Підходи до удосконалення державних механізмів боротьби з кіберзлочинностю 78

Оніщук В.С. Особливості введення психологічного впливу 80

Осьмак А.С. Цифрові голосові комунікації в публічному управлінні. Класифікація та безпека 82

Павленко М.М., Бондарчук А.А. Шляхи створення системи кібербезпеки України 84

Пилипчук В.Г. Проблеми та пріоритети розвитку правової науки в контексті цифрової трансформації, захисту прав та безпеки людини, суспільства і держави 87

Полотай О.І., Масюк Н.А. Профілі можливостей порушників інформаційної безпеки структурних підрозділів безпекових структур 92

Польовий М.А. Технологічні проблеми автоматичного виявлення проросійської пропаганди в мережі Facebook..... 96

Попутніков В.Б. Забезпечення інформаційної безпеки в процесі конфіденційного співробітництва 99

Потій О.В., Дубов Д.В., Семенченко А.І., Фіщук В.В. Організаційно-технічна модель кіберзахисту України..... 101

Прима А.М. Інформаційне забезпечення заходів протидії інформаційному впливу російській пропаганді..... 102

Прокопенко Є.М., Сівоха І.М. Пріоритети розвитку системи стратегічних комунікацій сектора безпеки і оборони України..... 104

Пучков О.О., Конюшок С.М. Освіта і просвіта у сфері кібербезпеки – завдання проєкту стратегії кібербезпеки України (2021–2025 роки)..... 107

Романов М.С. Щодо заходів в Україні з протидії гібридному впливу Російської Федерації 110

Сальнікова О.Ф., Іжутова І.В. Актуальні проблеми розвитку системи інформаційної безпеки..... 112

Самчишин О.В., Носова Г.Д. Перспективи розвитку системи кібернетичної безпеки України..... 113

Саричев Ю.О., Ткаченко В.А., Зубков В.П. Захист інформаційних ресурсів в системі державного управління у воєнній сфері..... 115

Сергієнко О.П. Шляхи підвищення ефективності захисту об’єктів інформаційної інфраструктури держави..... 117

Скачек Л.М. Інформаційна безпека як складова національної безпеки 119

Сніцаренко П.М., Саричев Ю.О., Грицюк В.В. Захист інформаційних ресурсів як елемент забезпечення інформаційної безпеки у воєнній сфері..... 121

Солодка О.М. Інформаційний суверенітет держави – імператив інформаційного суспільства..... 123

Тимофеєв А.О. Електронне досудове розслідування як один з напрямків розвитку інформаційної безпеки України 126

Тищенко Є.Ф. Щодо активізації діяльності СБ України у висвітленні результатів контррозвідувального захисту національної безпеки держави в інформаційній сфері 128

Ткачук Н.А. Щодо підготовки нової редакції Стратегії кібербезпеки України 130

Ткачук Н.І. Методологічні аспекти зарубіжного досвіду оцінювання ризиків і загроз у сфері національної безпеки 132

Ткачук Т.Ю. Онтологічні засади інформаційної безпеки держави 134

Толюпа С.В., Браіловський М.М., Штаненко С.С. Побудова систем виявлення вторгнень на основі методів DATA MINING 136

Федорієнко В.А. Особливості управління кібер-ризиками при побудові інформаційної інфраструктури Міністерства оборони України 138

Фурашев В.М. До пріоритетних напрямів розвитку системи інформаційної безпеки на період до 2030 року 140

Хлапонін Ю.І., Козубцова Л.М., Козубцов І.М. Про один з пріоритетних напрямків науково-обґрунтованого супроводження розвитку забезпечення кібернетичної безпеки 143

Черниш Р.Ф. Єдиний інформаційний простір системи безпеки громад: позитивні та негативні аспекти функціонування 145

Чеховська М.М., Гребенюк В.М. Гендерні аспекти гібридної війни російської федерації проти України 147

Шарий О.В. Розвідувальні органи України в системі забезпечення інформаціної безпеки держави 150

Шевченко О.А. Економічна та інформаційна безпека – пріоритетні напрямки забезпечення національної безпеки України в умовах євроінтеграції 152

Шидлюх В.В., Руснак С.О. Взаємодія як елемент стратегічних комунікацій 153

Шлапаченко В.М. Розвідувальна таємниця: проблемні питання запровадження нового виду таємної інформації 155

Штоквиш О.А. Маніпулювання історичною свідомістю як складова гібридної війни 158

Шуклін Г.В. Проблема моделювання керуванням інформаційною безпекою держави в умовах інформаційної експансії..... 160

Якименко Ю.М. Методичні підходи системного аналізу до вирішення проблем управління інформаційною безпекою в системі національної безпеки держави 162

ОРГАНІЗАЦІЙНО-ПРАВОВІ ПРОБЛЕМИ ЗАХИСТУ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Ахрамович В.М. Розробка методу розрахунку захисту інформації від репутації користувачів при нелінійній залежності параметрів..... 165

Бакалинський О.О., Пахольченко Д.В., Сапожнік Т.М. Аналіз забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури 167

Бондаренко І.П. Нормативне врегулювання питань створення систем інформаційної та кібербезпеки держави, аналіз та пропозиції 170

Бондарчук С.В., Галаган В.І. Деякі особливості процесу автентифікації та авторизації на сучасних аналітичних платформах..... 172

Гуз А.М. Основні етапи становлення системи кіберзахисту в Павнічноатлантичному альянсі на початку XXI ст. 174

Дашковська О.В., Погребняк В.П. Модернізація вищої освіти в Україні: євроінтеграційний аспект 176

Дзюба Т.М., Деркаченко Я.А., Опанасенко М.І. Обґрунтування концептуальних підходів до забезпечення інформаційної безпеки України..... 179

Дудикевич В.Б., Микитин Г.В., Галунець М.О. Організаційні-технічні аспекти проблеми кібербезпеки об’єктів критичної інфраструктури України 181

Ігнатушко Ю.І. Призначення інформаційної підсистеми «Custody records» 182

Кацалап В.О. Характеристика основних об’єктів критичної інформаційної інфраструктури України 184

Козюра В.Д., Бровко В.Д. Особливості сучасних кібератак 187

Котенко А.М., Гребенніков А.Б. Підвищення ефективності захисту кібернетичної безпеки об’єкту інформаційної діяльності 190

Котович В.М. Етичне тестування на злом та проникнення 192

Криворучко О.В., Десятко А.М., Сунічук О.М. Моделювання ІУС незалежного аудиту інформаційної безпеки 195

Крючкова Л.П., Вовк М.О. Дослідження параметрів прицільних завадових сигналів для захисту інформації на об’єктах критичної інфраструктури 197

Крючкова Л.П., Тарасенко Д.О. Інформаційне та алгоритмічне забезпечення ситуаційного управління на об’єктах критичної інфраструктури в умовах деструктивних впливів 199

Крючкова Л.П., **Українець Є.О.** Дослідження побічних електромагнітних випромінювань інтерфейсу USB в структурі систем управління об’єктами критичної інфраструктури 201

Легомінова С.В. Аспекти кіберстійкісті об’єктів критичної інфраструктури на прикладі США 204

Метелев О.П. Інформаційний простір як складова забезпечення інформаційної безпеки: проблема визначення юрисдикції 206

Мілих Є.Г. Методика оцінювання заходів забезпечення безпеки об’єктів критичної інформаційної інфраструктури 208

Моклякова К.П., Бабенко Т.В., Бігдан А.М., Ігніска В.І. Моделі оцінювання професійних компетенцій аудиторів 210

Мужанова Т.М. Індикатори інсайдерів відповідно до концепції CERT 213

Ожеван М.А. Геополітичні виклики глобальних інфодемічних війн 215

Порохня І.М., Рахімов В.В. Аналіз використання глобальних кібермереж для викрадення інформації 218

Савченко В.А., Лаптєв О.А., Кітура О.В. Виявлення інсайдерських загроз на основі інтелектуального аналізу журналів активності користувачів 220

Сапожнік Т.М., Пахольченко Д.В., Бакалинський О.О. Проблеми забезпечення кіберзахисту АСУ ТП 222

Тимошенко Р.Р., Загородніх В.В., Войтех К.Р. Деякі аспекти ієрархічної системи протидії кіберзагрозам у Збройних Сил України 225

Цмоканич І.В., Крючкова Л.П. Захист інформації від високочастотного нав'язування на об'єктах критичної інфраструктури 227

Цурко Ю.В. Фактори, які впливають на стан кібербезпеки об'єктів критичної інфраструктури 229

Штонда Р.М. Алгоритм дії адміністратора безпеки у разі виявлення в інформаційно-телекомунікаційних системах вірусу шифрувальника 231

Ящук В.І. Проектування автоматизованих інформаційних систем управління кібернетичною безпекою об'єктів критичної інфраструктури України 233

НАУКОВЕ МАЙБУТТЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ ОЧИМА МОЛОДИХ ВЧЕНИХ, СТУДЕНТІВ, КУРСАНТІВ

Березньова А.О. Корупція як загроза національній безпеці України 236

Бржевська З.М. Узагальнення моделі оцінки ризиків порушення достовірності інформації 238

Вансович Д.В., Фурсенко Д.Г. Сучасні виклики інформаційній безпеці держави в умовах цифрової трансформації 241

Відьменко Т.Є., Поліщук Д.В. Формування позитивного іміджу України в умовах ведення гібридної війни 243

Воробчук К.М., Шепета О.В. Актуальні проблеми управління інформаційною безпекою держави в умовах інформаційного протиборства 245

Гаврилюк Я.М. Аналіз державної політики забезпечення інформаційної безпеки України 247

Гайдай В.І. Наповнення місцевих бюджетів: інформаційна складова 249

Гальчинський Л.Ю., Горобець А.М. Оцінювання рівня спроможності персоналу об'єктів критичної інфраструктури до захисту від кіберзагроз 251

Горбатюк П.М. Напрями забезпечення громадського порядку органами сектору безпеки України 254

Гук О.М. Захист інформації в державних розподілених інформаційних системах в умовах кібервпливу противника 255

Даценко А.Ю. Щодо оцінки ефективності протидії дезінформації та пропаганді в умовах інформаційної війни 257

Дяченко С.А. Актуальність розробки методики адаптивного управління параметрами військових радіомереж 260

Єремеєва А.М., Тугарова О.К. Економічна складова інформаційної безпеки держави в умовах пандемії 262

Єсін О.В. Антиукраїнська інформаційно-пропагандистська кампанія на російському телебаченні 264

Загребельний В.С., Хмельницький О.О. Новітні методи спеціальних інформаційних операцій 265

Заскока Ю.В. Проблеми забезпечення кібербезпеки об'єктів критичної інфраструктури України 267

Ільїн Д.В., Фараон С.І. Використання пристроїв аутентифікації для підвищення рівня кібербезпеки об'єктів інформаційної критичної інфраструктури 269

Ільїн Р.О., Розвадовський О.Б. Вплив коронавірусу на кібербезпеку .. 271

Ісайко Д.І. Інформаційна війна 273

Канарський В.С. Пріоритети державної політики інформаційної безпеки України 275

Кириченко Є.О. Форми і засоби ведення інформаційної боротьби 277

Ковтун А.О. Дефініція «інформаційна безпека» та її місце в системі національної безпеки 279

Котляров Д.П., Семеній Д.М. Нормативно-правові засади забезпечення кібербезпеки України 281

Кудик П.О. Роль пропаганди і контрпропаганди під час ведення гібридної війни 283

Кульбачний М.С. Інформаційна безпека: проблеми та шляхи їх вирішення 285

Ласкевич А.Р. Організаційно-правові проблеми захисту кібернетичної безпеки 288

Липний С.І., Шепета О.В. Інформаційна безпека як складова національної безпеки в законодавстві україни: реальність і перспективи 290

Лоза В.В. Кібербезпека інформаційно-телекомунікаційних систем в умовах «індустрії 4.0» 291

Олійник І.О. Загальні проблеми захисту кібернетичного простору України 293

Омельян О.С. Щодо проблеми формування понятійно-термінологічного апарату у сфері кібербезпеки 296

Петренко К.М. Оцінювання інформаційних загроз державі у воєнній сфері 298

Прогонюк М.С., Благодарний А.М. Удосконалення правової регламентації державно-приватної взаємодії у сфері забезпечення кібербезпеки об'єктів критичної інфраструктури України 300

Прозоров А.Ю. Окремі аспекти співпраці Україна-НАТО у сфері з захисту інформації 302

Решетніков Д.І. Кіберзлочинність як загроза інформаційній безпеці України 305

Саакянц І.О. Міжнародні стандарти управління інформаційною безпекою та можливості їх застосування для вдосконалення системи захисту інформації в службі безпеки України 307

Савіцька В.І., Гоц О.В. Державна стратегія деокупації Криму: що буде далі? 309

Семеній Д.М., Котляров Д.П. Соціальна інженерія як загроза інформаційній безпеці 311

Семенчук М.Р. Використання технології ГІС для забезпечення військових та миротворчих операцій у світі 313

Толок Ю.С. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки України 315

Уткін Г.А. Гібридна війна – форма сучасного конфлікту держав 317

Фасоль О.О. Пріоритети розвитку національної безпеки на період до 2030 року 319

Федоров І.А. Програмно апаратний симулятор інфраструктури компаній 321

Холдоєнко А.В. Інформаційна безпека в контексті національної безпеки 323

Шилов М.С., Жевелєва І.С. Удосконалення системи управління інформаційною безпекою в організаціях..... 325

Шнайдерський І.С. Окремі питання правового статусу Президента України із забезпечення національної безпеки і оборони України 327

Юрчак І.І. Управління інцидентами інформаційної безпеки 329

Рекомендації
науково-практичної конференції: “Актуальні проблеми управління інформаційною безпекою держави”..... 332

Наукове видання

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

XII Всеукраїнська науково-практична конференція

Збірник тез наукових доповідей
(Київ, 26 березня 2021 року)

Електронне видання

Авторська редакція

Технічне редагування, макетування *Т. О. Коркач*

Видавець і виготовлювач
Національна академія Служби безпеки України,
03066, Київ, вул. Михайла Максимовича, буд. 22.
факс: (044)257-30-35
E-mail: academy@ssu.gov.ua
Свідоцтво суб'єкта видавничої справи ДК № 6844 від 17.07.2019.