ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ ТА ВИДИ ДЖЕРЕЛ ЗАГРОЗ І НЕБЕЗПЕК

Курсант Н.В. Чудінова;
проф. Ю.І. Грицюк, д-р техн. наук – Львівський ДУ БЖД

Вступ. Інтереси держави в інформаційній сфері в основному зводяться до гармонійного розвитку інформаційної структури держави. Інформаційна безпека держави[1] – це стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає істотної шкоди національним інтересам.

Проте, ще досі не прийнято закону, який би визначав концепцію державної інформаційної політики України. Відповідно, в країні не існує єдиного плану, єдиної державної позиції чи стратегії розвитку інформаційної галузі, а отже і забезпечення інформаційної безпеки. Протягом 2002-2010 рр. було три спроби ухвали концепцію державної інформаційної політики – 2002, 2009 та 2010 року. 11 січня 2011 року черговий проект концепції прийняли у першому читанні за основу закону і направили на доопрацювання Комітету Верховної Ради України з питань свободи слова та інформації[2].

Ще дотепер вважається, що загрози інтересам держави можуть проявлятися тільки у вигляді отримання зловмисниками протиправного доступу до відомостей, що становлять державну таємницю, до іншої конфіденційної інформації, розкриття якої може нанести збитки державі. Також вважається, що найбільш небезпечними джерелами загроз інтересам держави в інформаційному суспільстві є неконтрольоване розповсюдження інформаційної зброї, спроби реалізації концепції ведення інформаційних війн.

Отож, мета роботи полягає у визначенні інформаційної безпеки України, аналізі сучасних джерел загроз, причин їх виникнення та наслідків реалізації. Основними завданнями роботи є: розгляд причин появи інформаційних війн і їх особливостей; характеристика видів джерел загроз і небезпек національним інтересам і безпеці в інформаційній сфері.

Інформаційна безпека у структурі національної безпеки України. Відповідно до законодавства України, поняття "інформаційна безпека" має таке визначення[3]: "стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди державі через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних

---

[1] http://uk.wikipedia.org/wiki/Інформаційна_безпека_України

[2] Постанова Верховної Ради України "Про прийняття за основу проекту Закону України про Концепцію державної інформаційної політики". [Електронний ресурс]. – Доступний з http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2897-17.

[3] Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" // Відомості Верховної Ради України (ВВР), 2007 р., № 12, ст. 102.

технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації".

Виокремлюють три рівня забезпечення інформаційної безпеки[4]: рівень особи (формування раціонального, критичного мислення на основі принципів свободи вибору); суспільний рівень (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам); державний рівень (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам).

Національні інтереси України в інформаційній сфері вирізняють такі життєво важливі інтереси: недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур; ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригуванні державної політики в інформаційній сфері; побудова та розвиток інформаційного суспільства; забезпечення економічного та науково-технологічного розвитку України; формування позитивного іміджу України; інтеграція України у світовий інформаційний простір.

Принципи забезпечення інформаційної безпеки України зводяться до такого: свобода збирання, зберігання, використання та поширення інформації; достовірність, повнота та неупередженість інформації; обмеження доступу до інформації виключно на підставі закону; гармонізація особистих, суспільних і державних інтересів; запобігання правопорушенням в інформаційній сфері; економічна доцільність; гармонізація українського законодавства в інформаційній сфері з міжнародним; пріоритетність національної інформаційної продукції.

Інформаційні війни та їх особливості. Вперше термін "інформаційна війна" з'явився наприкінці 80-х років XX століття. Він став результатом плідної праці теоретиків збройних сил США, почав широко використовуватися після вдало проведеної роботи зі знищення СРСР. На сьогодні саме інформаційні війни становлять найбільшу небезпеку нормальному функціонуванню системи органів державного управління.

Відомі два трактування поняття "інформаційні війни": гуманітарне і технічне. У гуманітарному розумінні інформаційна війна представляє собою активні методи перетворювання інформаційного простору, тобто нав'язування громадянам України таких моделей суспільства, які забезпечують бажані типи поведінки, а також породжують інформаційні процеси міркувань.

Інформаційна війна при використанні інформації як зброї ведення бойових дій у будь-якій сфері життєдіяльності містить такі складові:

---

[4] Кузьменко А.М. Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного протиборства / А.М. Кузьменко // Часопис Київського університету права. – 2010. – № 4. – С. 317-321.

- *здійснення впливу на інфраструктуру систем життєзабезпечення* – телекомунікації, транспортні мережі, електростанції тощо;
- *промисловий шпіонаж* – порушення прав інтелектуальної власності, розкрадання патентованої інформації, викривлення або знищення важливих даних, проведення конкурентної розвідки;
- *хакінг* – зламування та використання особистих даних, ідентифікаційних номерів, інформації з обмеженим доступом тощо.

Існує декілька підвидів інформаційних воєн:

- *кібервійна* – комп'ютерне протистояння у просторі мережі Інтернет, спрямоване на дестабілізацію комп'ютерних систем державних установ, фінансових і ділових центрів, створення безладу та хаосу в житті країни;
- *мережева війна* – форма ведення конфліктів, коли її учасники застосовують мережеві стратегії та технології, пристосовані до сучасної інформаційної доби. Учасниками таких воєн можуть бути терористи, кримінальні угруповання, громадські організації та соціальні рухи, які використовують децентралізацію комп'ютерних систем;
- *електронна війна* – використання та управління інформацією з метою набуття переваги конкурента над супротивником, здійснює збирання тактичної інформації, забезпечує безпеку власних інформаційних ресурсів, поширює неправдиву інформацію про ворога і населення, перешкоджає збиранню інформації супротивником;
- *психологічна війна* – сукупність різних форм, методів і засобів впливу на людину з метою зміни в бажаному напрямку її психологічних характеристик, групових норм поведінки, масових настроїв, суспільної свідомості загалом;
- *радіоелектронна боротьба* – сукупність узгоджених за цілями, задачами, місцем і часом заходів і дій військ, спрямованих на здобування інформації про місцезнаходження радіоелектронних засобів, систем управління військами і зброї суперника, їх знищення всіма видами зброї, а також радіоелектронному подавленню сигналів передачі інформації.

Отже, поняття інформаційна війна – це дії, що здійснюються для досягнення інформаційної переваги власної воєнної стратегії через вплив на інформацію та комунікаційні системи суперника при одночасному забезпеченні безпеки власних інформаційних ресурсів. Одним з прикладів є вказівка спецслужб США відстежувати телефонні розмови, що виходять за її межі. За допомогою відповідної програми усі телефонні дзвінки записуються, а потім пропускаються через спеціальну апаратуру, яка за допомогою пошукових систем за ключовими словами виявляє та ідентифікує важливу інформацію.

Основна мета сучасної інформаційної війни полягає не у фізичному знищенні суперника та ліквідації його збройних сил, а у широкомасштабному порушенні роботи фінансових, транспортних і комунікаційних мереж і систем, у руйнуванні економічної інфраструктури і підкоренні населення країни, що зазнала атаки, волі країни-переможця.

Основним інструментом ведення інформаційної війни є інформаційна зброя, тобто пристрої та засоби, які призначені для нанесення протидіючій стороні максимальної шкоди в ході інформаційної боротьби. Основними елементами інформаційної боротьби є:

- засоби інформаційно-технічного характеру, які знищують, перекручують або викрадають інформацію, не зважаючи на систему захисту, обмеження доступу до цієї інформації законних користувачів;
- інформаційно-психологічні засоби, які дезорганізують інформаційні системи шляхом дезінформації, формування помилкових логічних інформаційних концепцій, інтерпретацій та ін., впливаючи таким чином на суспільну думку, на життя суспільства, держави або групи держав загалом.

Інформаційна зброя є інструментом встановлення контролю над інформаційними ресурсами потенційного суперника, тому вона втручається в роботу систем управління та інформаційних систем, систем зв'язку, з метою порушення їх працездатності аж до цілковитого виведення їх з ладу, вилучення, перекручення даних, які в них містяться, або цілеспрямованого введення спеціальної інформації. Здебільшого інформаційна зброя розповсюджує дезінформацію в системі формування суспільної свідомості й прийняття рішень. Особливу небезпеку в цьому випадку становлять дані, що надходять для органів державної влади, оскільки від їх достовірності залежить здатність цих органів приймати правильні рішення та вживати своєчасні заходи з управління державою.

Інформаційна зброя враховує різні варіанти протидії, тому чим більше таких варіантів ураховано, тим більша ймовірність успіху в тій чи іншій інформаційній агресії. *Інформаційне протиборство* – форма боротьби сторін в інформаційному просторі з використанням політичних, економічних, дипломатичних, військових та інших методів, способів та засобів для впливу на інформаційне поле суперника та захисту власного інформаційного поля в інтересах досягнення поставлених цілей. На сьогодні відомі такі сфери протиборства: світоглядна, політична, дипломатична, воєнна, науково-технологічна, соціальна та гуманітарна, ідеологічна, екологічна тощо.

Інформаційна війна має наступальні та оборонні складові, починаючи з цільового проектування та розроблення своєї структури командування, управління, комунікацій комп'ютерів і розвідки. Вона може бути спрямована проти трьох елементів інфраструктури: комп'ютерів; програмного забезпечення; людини. Однією з головних цілей та завдань інформаційної війни є придушення в людині морального творчого початку, зміна власного світогляду. На міжнародній арені інформаційні війни ведуться:

- між державами та блоками держав;
- між міжнародними корпораціями, транснаціональними компаніями і міжнародними фінансовими групами з державами;
- між терористичними організаціями та державами;
- між злочинними організаціями;
- між злочинними організаціями та державами.

Загалом сучасні інформаційні технології певною мірою зрівняли індустріальні, постіндустріальні та доіндустріальні країни: всі вони мають доступ до інструментарію, необхідного для ведення інформаційної війни, а отже виступають як суб'єкти, так і об'єкти інформаційної війни і, як наслідок, забезпечення внутрішньої інформаційної безпеки.

Таким чином, інформаційна війна використовує переваги технологічних вдосконалень, вона вже настільки близько підійшла до практичної реалізації,

що подальше нехтування цим питанням просто недопустиме. Зброєю в цьому напрямку боротьби є пристрої та технології, які використовуються для широкомасштабного, цілеспрямованого, швидкого та таємного впливу на цивільні та військові інформаційні системи суперника.

Види джерел загроз інформаційній безпеці України. Однією з основних загроз інформаційній безпеці Закон України "Про основи національної безпеки"[5] називає "намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації". До інших загроз віднесено: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави.

В "Доктрині інформаційної безпеки України"[6], підписаній Президентом в липні 25.05.2009 р., серед всього виділено такі загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет; деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності України; прояви сепаратизму в засобах масової інформації, а також у мережі Інтернет, за етнічною, мовною, релігійною та іншими ознаками.

Таким чином, поняття "загроза інформаційній безпеці" визначається:

1) відсутністю єдиного підходу до дослідження основних понять інформаційної безпеки;
2) недостатньою розробленістю початкового поняття "загроза" і питань його відмежування від інших споріднених понять, таких як "небезпека", "виклик", "ризик", і відповідно видового "інформаційна загроза" і його відмежування від таких понять, як "інформаційна війна", "інформаційне протиборство", "інформаційний тероризм";
3) наявністю невирішеної проблеми формування категорійно-понятійного апарату теорії інформаційної безпеки;
4) можливістю на підставі теоретичних розробок цього апарату формувати адекватну систему моніторингу та управління джерелами загроз та рівнем їх небезпеки в інформаційній сфері.

Загрози інформаційним ресурсам держави можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, що зберігається в ній. Виникнення загрози, тобто виявлення дже-

---

[5] Закон України "Про основи національної безпеки України" // Відомості Верховної Ради України (ВВР). – 2003. – № 39, ст. 351. [Електронний ресурс]. – Доступний з http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=964-15.

[6] РНБОУ оприлюднила "Проект Доктрини інформаційної безпеки України" (+текст). [Електронний ресурс]. – Доступний з http://www.telekritika.ua/news/2009-05-25/45781

рел актуалізації певних подій у реалізації загрози інформаційним ресурсам характеризується таким елементом як уразливість. Саме за наявності вразливості як певної характеристики системи і відбувається активізація джерел загроз і небезпек.

Згідно з Законом України "Про основи національної безпеки України", до джерел загроз і небезпек національним інтересам і національній безпеці в інформаційній сфері належать:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу таємницю, передбачену законом, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів особи, суспільства та держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

До джерел загроз і небезпек інформаційній безпеці системі управління національною безпекою належать: розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання.

Отож, як інформаційні війни, так і інформаційне протиборство й інформаційна боротьба є проявами одного більш широкого поняття – загрози національним інтересам і національній безпеці в інформаційній сфері.

Висновок. Вибір цілей і методів протидії конкретним загрозам та небезпекам у сфері інформаційної безпеки України становить важливу проблему і складову частину діяльності по реалізації основних напрямів державної політики інформаційної безпеки. У межах вирішення даної проблеми визначаються можливі форми відповідної діяльності органів державної влади, що потребує проведення детального аналізу економічного, соціального, політичного та інших станів суспільства, держави і особи, можливих наслідків вибору тих чи інших варіантів здійснення цієї діяльності.

Література

1. Попов М.О. До забезпечення воєнної безпеки в умовах загрози інформаційної війни / М.О. Попов, А.Г. Лук'янець // Наука і оборона : наук.-теорет. та наук.-практ. журнал. – 1999. – № 2. – С. 37-43.

2. Сідак В.С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник / В.С. Сідак, В.Ю. Артемов. – К. : Вид-во КНТ, 2007. – 21-24 с.

3. Харченко В.С. Інформаційна безпека : глосарій / В.С. Харченко. – К. : Вид-во КНТ, 2005. – 13-18 с.

4. Цимбалюк В.С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. : Вид-во НТУ України "КПІ", 2001. – № 4. – С. 43-48.