7. Постанова Апеляційного суду м. Києва від 29 травня 2018 р., судова справа № 761/4115/16-ц. URL: http://reyestr.court.gov.ua/Review/74535048 (дата звернення: 22.11.2018).

8. Ухвала Верховного суду від 20 липня 2018 року. Справа № 761/4115/16-ц. URL: http://reyestr.court.gov.ua/Review/75498131 (дата звернення: 22.11.2018).

9. Доповідь «Про верховенство права», п. 37: Венеціанська комісія, 22-26 березня 2011 р. URL: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2011)003rev-rus (дата звернення: 22.11.2018).

Ліщук Ю.Г., Мороз Д.А.
студенти,
Науковий керівник: **Ярош А.О.**
кандидат юридичних наук, доцент,
Університет державної фіскальної служби України

ІНФОРМАЦІЙНА БЕЗПЕКА ТА МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Інтенсивна інформатизація всіх сфер життєдіяльності суспільства нині є одним із визначальних глобальних чинників подальшого соціально-економічного, інтелектуального та духовного розвитку людства. Водночас людство вступає в нову еру розвитку, котра може бути охарактеризована як період інформаційних воєн. Зокрема, інформаційний складник становить ключовий елемент гібридної війни проти України, що створює реальні загрози національній безпеці. Відтак за умови швидкого формування й розвитку інформаційного суспільства в Україні особливого значення набуває проблема інформаційної безпеки [1].

Дослідження інформаційної безпеки в складі державної інформаційної політики припускає вирішення цілого комплексу питань загальнонаукової властивості. При цьому важливим стає не лише з'ясування сутнісних рис, функцій державної інформаційної політики в області інформаційної безпеки, але і виявлення основних чинників, що впливають на неї. Цьому присвячені різнопланові праці А. В. Герасімова, О. Н. Забузова, Б. В. Коваленко, А.В. Костіна, А. А. Кочеткова, В. Ф. Коломійця, А. В. Манойло, А. І. Марущака, С. А. Модестова, В. Ф. Ніцевіча, О. В. Олійника, О. В. Сосніна, Н. Н. Панаріна, А. І. Пірогова, А. І. Позднякова, Г. Г. Почепцова та ін.

Згідно Доктрини інформаційної безпеки [2], інформаційна безпека України, як невід'ємна складова сфери національної безпеки, є комплекс соціально-економічних, морально-політичних, духовно-ідеологічних і військово-стратегічних ініціатив, що підкоряються жорсткій логіці державних інтересів. У Концепції національної безпеки України [3] та Законі України «Про основи національної безпеки» [4] розглядаються основні напрямки забезпечення безпеки в інформаційній сфері, під якою часто розуміють інформаційну безпеку як складову національної безпеки України.

Аналіз поглядів і концептуальних підходів до формування сучасних ефективних систем інформаційної безпеки дозволив сформулювати основні функції та завдання і намітити організаційні основи функціонування відповідних підрозділів інформаційної безпеки.

У сучасному поданні рольових функцій служби інформаційної безпеки можна виділити чотири напрями [5]:

1) розробка методології та методик аналізу загроз, оцінки рівня інформаційної безпеки і системи її забезпечення;

2) організація і здійснення конкретних видів діяльності із захисту інформації; 3) експлуатація технічних засобів захисту інформації;

3) аудит і контроль функціонування системи інформаційної безпеки об'єктів [6, с. 131].

Завдання забезпечення інформаційної безпеки необхідно вирішувати системно.

Технології захисту даних повинні ґрунтуються на застосуванні сучасних методів, які запобігають витоку інформації та її втраті.

Сьогодні використовується шість основних способів захисту: перешкода, маскування, регламентація, управління, примус, спонукання. Усі перераховані методи націлені на побудову ефективної технології захисту інформації, при якій виключено витрати через недбалість і успішно відображено різні види загроз. Під перешкодою розуміється спосіб фізичного захисту інформаційних систем, завдяки якому зловмисники не мають можливості потрапити на територію, що охороняється.

Маскування – способи захисту інформації, що передбачає перетворення даних у форму, не придатну для сприйняття сторонніми особами. Для розшифровки потрібне знання принципу.

Управління – способи захисту інформації, при яких здійснюється управління над всіма компонентами інформаційної системи.

Регламентація – найважливіший метод захисту інформаційних систем, що припускає введення особливих інструкцій, згідно з якими повинні здійснюватися всі маніпуляції з даними, що охороняються.

Примус – методи захисту інформації, тісно пов'язані з регламентацією, що припускають введення комплексу заходів, при яких працівники змушені виконувати встановлені правила [7].

Способи захисту інформації передбачають використання певного набору засобів. Для запобігання втрати та витоку таємних даних використовуються засоби:

– фізичні;
– апаратні;
– програмні;
– апаратно-програмні;
– законодавчі;
– криптографічні та організаційні методи [8].

Для того, щоб створити ефективну систему інформаційної безпеки України, необхідно, на наш погляд, виконати два кроки. По-перше, запровадити відповідне законодавче рішення. По-друге, об'єднати у цьому напрямі дослідження науковців, досвід практиків і зусилля Ради національної безпеки і оборони України. Саме РНБО на початковому етапі має стати об'єднавчою структурою для всіх учасників процесу формування системи інформаційної безпеки. Таким чином, інтенсивний пошук шляхів забезпечення інформаційної безпеки України і, в першу чергу, виявлення інформаційно-психологічного впливу на населення України та кібер нетичних атак на державні й відомчі інформаційні ресурси є важливим питанням вітчизняної науки. Порушені проблеми повинні виноситися на розгляд спеціалістів і науковців в означеній сфері з метою спільного пошуку шляхів їх вирішення в інтересах надійного забезпечення національної безпеки нашої держави.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України : Указ Президента України від 15.03.2016 № 96/2016 [Електронний ресурс]. – Режим доступу: www.president.gov.ua/ documents/962016-19836.

2. Указ Президента України «Про Доктрину інформаційної безпеки України» від 8.07.2009 р. № 514/2009.

3. 3.Про Концепцію (основи державної політики) національної безпеки України : Постанова Верховної Ради України від 18.07.1995 р. № 532-95-п (Із змінами, внесеними згідно з Постановою КМ № 1849 (1849-98-п) від 23.11.1998 р.) // Відомості Верховної Ради України. – 1997. – № 10. – Ст. 85.

4. Закон України «Про основи національної безпеки України» // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

5. Іванов О. В. Інформаційна складова сучасних війн / О. В. Іванов //Вид. Моск. ун-та: сер. 18 : Соціологія і політологія. – 2004. – № 4. – С. 64-70.

6. Марунич А. В. Захист інформації як основна складова економічної безпеки підприємства / А. В. Марунич // Управління розвитком. – 2014. – № 14. – С. 130-132.

7. 7.Ясенєв В. Н. Інформаційна безпека в економічних установах: підручник. [Электронный ресурс] / В. Н. Ясенєв. – Н. Новгород : Вид.ННГУ, 2006. – Режим доступу: http://ebib.pp.ua/informatsionnaya-bezopasnost-ekonomicheskih88.html.

8. Захаркін О. О. Інформаційні системи та технології у фінансових установах : конспект лекцій [Електронний ресурс] / О. О. Захаркін, М. Ю. Абрамчук, М. А. Деркач. – Суми : Вид-во СумДУ, 2007. – 80 с. – Режим доступу: http://elkniga.info/book_188.htm