DOI 10.52363/2414-5866-2023-2-47
УДК 321.6.8

Садковий В.П., *д.держ.упр., проф., НУЦЗУ, м. Харків,*
ORCID: 0000-0001-7054-671X,
Клочко А.М., *д.ю.н., проф., ХНУВС, м. Харків,*
ORCID: 0000-0002-6898-964X,
Борисова Л.В., *к.ю.н., доц., НУЦЗУ, м. Харків,*
ORCID: 0000-0001-6554-1949,
Нікітіна Л.О., *к.т.н., доц., НТУ «ХПІ», м. Харків,*
ORCID: 0000-0001-9175-6716,
Коломієць В.С., *НУЦЗУ, м. Харків, ORCID: 0009-0001-4058-4026*

Sadkovy V., *Doctor of Public Administration, Professor,*
National University of Civil Protection of Ukraine, Kharkiv,
Klochko A., *Doctor in Law Sciences, Professor, Kharkiv National University of Internal Affairs, Kharkiv,*
Borysova L., *Ph.D in Law Sciences, Associate Professor,*
National University of Civil Protection of Ukraine, Kharkiv,
Nikitina L., *Ph. in Technical Sciences, Associate Professor,*
National Technical University "Kharkiv Polytechnic Institute", Kharkiv,
Kolomiets V., *National Technical University "Kharkiv Polytechnic Institute", Kharkiv*

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

STATE POLICY IN THE SPHERE OF TECHNICAL PROTECTION OF INFORMATION

У статті досліджуються питання наукової розробки проблеми державної політики у сфері технічного захисту інформації, питання організаційних, правових і технічних заходів захисту інформації. Сформульовані основні напрями реалізації державної політики щодо захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах та шляхи виконання низки заходів відповідно до визначених завдань. Зазначено, що вимоги безпеки ідентифікуються систематичною оцінкою ризиків, які визначають відповідні управлінські дії та пріоритети управління ризиками інформаційної безпеки для забезпечення зниження ризиків до прийнятного рівня. Визначені принципи та основні напрями формування і проведення державної політики у сфері технічного захисту інформації для унеможливлення реалізації загрози для інформації. Звертається увага на підготовку і видання відповідних нормативно-правових актів та нормативних документів з урахуванням міжнародного досвіду. Зроблено висновок, що забезпе-

чити безпеку комп'ютерної інформації в телекомунікаційній мережі неможливо, так як абсолютно захищена система непридатна для її використання, крім того не всі шляхи подолання безпеки реально відомі.

Ключові слова: *державні інформаційні ресурси, державна політика у сфері технічного захисту інформації, захист інформаційних ресурсів, засоби технічного захисту інформації.*

The article examines issues of scientific development of the problem of state policy in the field of technical information protection, issues of organizational, legal and technical measures of information protection. The main directions of the implementation of the state policy regarding the protection of state information resources in information and telecommunication systems and the ways of implementing a number of measures in accordance with the defined tasks have been formulated. It is noted that security requirements are identified by systematic risk assessment, which determines appropriate management actions and information security risk management priorities to ensure risk reduction to an acceptable level. The principles and main directions of the formation and implementation of state policy in the field of technical protection of information to prevent the realization of threats to information are defined. Attention is drawn to the preparation and publication of relevant normative legal acts and normative documents taking into account international experience. It was concluded that it is impossible to ensure the security of computer information in the telecommunications network, since a completely secure system is unsuitable for its use, besides, not all ways of overcoming security are really known.

Keywords: *state information resources, state policy in the field of technical information protection, protection of information resources, means of technical information protection.*

Постановка проблеми. Загальноприйнятою особливістю та характеристикою інформаційного суспільства є наявність інформаційної інфраструктури, що складається з телекомунікаційних мереж та розподілених у них інформаційних ресурсів як запасів знань. Процеси перетворення та реалізації знань через матеріалізацію інформаційного ресурсу отримують розвиток за рахунок високих інформаційних технологій, що характеризується значною кількістю циркулюючої комунікаційними каналами зв'язку інформації, а також наявністю необхідних засобів її збереження, пересилання, оброблення, використання та захисту.

Термін «захист інформації» (англ. Data protection) визначає сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації. Безпека звичайно пов'язується зі станом нормального функціонування суспільних інститутів та інших форм соціальної діяльності, зі станом захищеності об'єкта (системи) від зовнішніх та внутрішніх негативних впливів, загроз, небезпек тощо. При цьому основними

об’єктами, на які направлені заходи із забезпечення безпеки, є людина і громадянин, суспільство і держава.

Проблема формування та реалізація державної політики у сфері технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту яких встановлена законом, актуалізується з урахуванням нових тенденцій, викликів і загроз у кіберпросторі, і тими ризиками, що з’являються через неможливість контролювати тенденції і процеси інформаційно-соціального та інформаційно-технологічного розвитку.

Аналіз останніх досліджень і публікацій. Питання захисту інформації, у тому числі державних інформаційних ресурсів, розкривали вітчизняні дослідники у розрізі своїх генеральних досліджень: О.Д. Довгань, В.А. Ліпкан, В.Г. Пилипчук, А.М. Гуз, Т.Ю. Ткачук, О.Б. Розвадовський, О.О. Пучков та інші. Ефективність діяльності державних органів у сфері захисту інформації України була предметом досліджень вчених А.І. Марущака, О.К. Юдіна, О.В. Сосніна. На думку Г. Почепцова, інформаційну політику необхідно розглядати як сукупність принципів, підходів, визначальних законів функціонування информаційної сфери [4, с. 12]. В.І. Абрамов, Г.П. Ситник, В.Ф. Смолянюк розглядають інформаційну політику держави як діяльність держави в інформаційній сфері, спрямовану на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору цілісної держави та його інтеграції у світовий інформаційний простір з урахуванням національних особливостей і інтересів під час забезпечення інформаційної безпеки на внутрішньо державному та міжнародному рівнях [5, с. 6].

Постановка завдання. Метою статті є обґрунтування пріоритетних завдань захисту інформації.

Виклад основного матеріалу. Науково-технічний прогрес встановив перед людством відповідальність за використання отриманої могутності – «розвиток техніки несе необмежені можливості для добра і зла» [3, с. 76].

Прогрес у різних галузях науки і техніки призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна підключатись до ліній телекомунікацій та різноманітних технічних засобів опрацювання інформації з метою здобування, пересилання та аналізу даних. Комунікаційне обладнання, яке використовується в мережах зв’язку, передбачає дистанційний доступ до його апаратних та програмних засобів, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв’язку та змістом повідомлень, які пересилаються. За таких умов створились можливості витоку інформації, порушення її цілісності та блокування.

Небезпека є об’єктивною і очевидною субстанцією, що має місце в реальній дійсності. Прагнення людини убезпечитися від загрожуючих чинників, явищ і процесів є природним і актуальним. Безпека, тобто стан захище-

ності життєво важливих інтересів громадянина, суспільства, держави, людства і цивілізації від небезпек, – це одна з найважливіших цінностей соціального буття людей, обов'язкова передумова існування і подальшого розвитку людства. Безпека повинна створювати гармонію і переборювати протиріччя у відносинах «людина – техніка», «техніка – техніка», «людина – навколишнє середовище», у взаєминах між людьми, особою і державою, суспільством, між націями і державами.

Реалізація державної політики щодо захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах полягає у:

– підготовці пропозицій до визначення загальної стратегії та пріоритетних напрямів діяльності у сфері захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

– виконанні обов'язків уповноваженого органу у сфері захисту інформації в інформаційно-телекомунікаційних системах;

– розробленні порядку та вимог до захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також погодження проектів нормативно-правових актів з цих питань;

– розробленні критеріїв та порядку оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо.

Реалізація державної політики забезпечується шляхом виконання низки заходів відповідно до визначених завдань, а саме:

– методичного керівництва та координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності з питань, пов'язаних із запобіганням вчиненню порушень безпеки інформації в інформаційно-телекомунікаційних системах, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

– накопичення та аналізу даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також про їх наслідки;

– організації та здійснення оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, надання відповідних рекомендацій.

Вважається (С.Е. Остапов, С.П. Євсеєв, О.Г. Король) , що система захисту інформації не може забезпечити стовідсотковий ефект. Відповідно, визначається певний рівень інформаційної безпеки, який відображає припустимий ризик її спотворення, знищення, несанкціонованого доступу та витоку. Таким чином, основне завдання захисту інформації полягає в тому, щоб злам системи відбувся якомога пізніше та/або не мав суттєвих наслідків для її функціонування й використання інформації, що нею циркулює.

Вимоги безпеки ідентифікуються систематичною оцінкою ризиків безпеки. Результати оцінки ризику визначають відповідні управлінські дії та пріоритети управління ризиками інформаційної безпеки і впровадження контролів, вибраних для забезпечення зниження ризиків до прийнятного рівня. Оцінка ризиків повинна періодично повторюватися для врахування змін, які можуть вплинути на результати оцінки ризику. Мета якісної оцінки ризиків – ранжувати інформаційні загрози та небезпеки за різними критеріями, система яких дозволить сформувати ефективну систему впливу на них. Для забезпечення інформаційної безпеки впроваджується відповідний набір контролів, який включає політику, процеси, процедури, організаційні структури і програмні та апаратні функції. Вибір контролів безпеки залежить від управлінських рішень, основаних на критеріях прийняття ризику, варіантах обробки ризику та загальному підході до управління ризиком, застосовному в організації, і повинен також відповідати усьому чинному національному й міжнародному законодавству та нормативним документам.

Отже, безпека, яка може бути досягнута за допомогою технічних засобів, є обмеженою і має підтримуватись відповідним управлінням та процедурами, що включають спеціальні технічні засоби та методи захисту інформації від несанкціонованого доступу.

Концепція технічного захисту інформації в Україні (Постанова Кабінету Міністрів України від 8 жовтня 1997 р. №1126) визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами. Технічний захист інформації (ТЗІ) є складовою частиною забезпечення національної безпеки України. Стратегія захисту інформації визначає основу для побудови комплексу заходів щодо інформаційної безпеки, передбачаючи необхідні, конкретні засоби захисту, які є найбільш дієвими з точки зору наявних інформаційних, фінансових та людських ресурсів. Напрями розвитку ТЗІ обумовлюються необхідністю своєчасного використання заходів, адекватних масштабам загроз для інформації, і ґрунтуються на засадах правової, соціальної, демократичної держави відповідно до прав суб'єктів інформаційних відносин на доступ до інформації та її захист.

Принципами формування і проведення державної політики у сфері технічного захисту інформації є:

– дотримання балансу інтересів особи, суспільства та держави, їх взаємна відповідальність;

– єдність підходів до забезпечення цього захисту, які визначаються загрозами безпеці інформації та режимом доступу до неї;

– комплексність, повнота та безперервність його заходів;

– відкритість нормативно-правових актів та нормативних документів з питань такого захисту, які не містять відомостей, що становлять державну таємницю тощо.

Основними напрямами державної політики у сфері технічного захисту

інформації, які зумовлені пріоритетністю національних інтересів і мають на меті унеможливлення реалізації загрози для інформації, виступають:

– її нормативно-правове забезпечення: удосконалення чинних та створення нових нормативно-правових актів щодо захисту інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що належить державі;

– розроблення нормативно-правових актів щодо захисту відкритої інформації, важливої для особи, суспільства та держави;

– удосконалення правових механізмів організаційного забезпечення технічного захисту інформації;

– удосконалення нормативно-правових актів щодо умов і правил провадження діяльності у сфері технічного захисту інформації;

– удосконалення нормативно-правових актів щодо здійснення контролю за імпортом з метою впровадження в Україні іноземних інформаційних технологій з захистом інформації тощо.

Приведення інформаційних відносин у сфері ТЗІ у відповідність із міжнародними стандартами сприятиме утвердженню України у світі як демократичної, соціальної, правової держави. Слід звернути увагу на важливе положення, що має бути покладене в основу формування системи захисту даних при міждержавній співпраці, оскільки гарантувати інформаційний суверенітет України при міжнародному інформаційному обміні без створення ефективної системи технічного захисту інформації практично неможливо.

Подальшим кроком у напрямку організації та здійснення оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах має стати підготовка та видання відповідних нормативно-правових актів та нормативних документів, які б, з урахуванням міжнародного досвіду, дозволили оптимізувати вироблення єдиних критеріїв та порядку такого оцінювання.

Обов'язковою умовою забезпечення захисту інформації, яка циркулює в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності, є одержання об'єктивної оцінки рівня захищеності інформації, що здійснюється шляхом проведення державної експертизи та атестації.

Перелік засобів ТЗІ формується відповідно до п. 17 Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 р. № 1229 і призначений для використання суб'єктами системи технічного захисту інформації (ТЗІ) під час розроблення, модернізації та впровадження комплексів ТЗІ на об’єктах інформаційної діяльності (ОІД) та комплексних систем захисту інформації (КСЗІ) в автоматизованих системах (АС).

Перелік містить номенклатуру засобів ТЗІ (технічних засобів, основним функціональним призначенням яких є захист інформації від загроз витоку, порушення цілісності та блокування; технічних засобів, в яких додат-

ково до основного призначення передбачено функції захисту інформації; засобів, які призначені, спеціально розроблені або пристосовані для пошуку закладних пристроїв і які створюють загрозу для інформації; засобів, які спеціально розроблені або пристосовані для оцінювання захищеності інформації), відповідність яких вимогам нормативних документів з питань ТЗІ засвідчено сертифікатом відповідності або позитивним експертним висновком, одержаними у порядку, який встановлено нормативно-правовими актами: Правилами проведення робіт із сертифікації засобів захисту інформації, затвердженими спільним наказом Адміністрації Держспецзв'язку та Держспоживстандарту України від 25.04.2007 р. № 75/91 та Положенням про державну експертизу в сфері технічного захисту інформації, затвердженим наказом Адміністрації Держспецзв'язку України від 16.05.2007 р. № 93.

Використання засобів цього Переліку під час створення, модернізації та впровадження комплексів ТЗІ на ОІД та КСЗІ в АС не увільняє від необхідності оцінювання відповідності досягнутого рівня захисту інформації встановленому вимогами нормативних документів з ТЗІ, яке здійснюється шляхом атестації комплексів ТЗІ на ОІД або експертизи КСЗІ в АС.

Модернізація засобів ТЗІ в комп’ютерних системах здійснюється у відповідності з окремим ТЗ або доповненням до основного ТЗ на створення засобу ТЗІ. ТЗ (доповнення до основного ТЗ) розробляється та оформляється відповідно до чинних ДСТУ з урахуванням вимог НД ТЗІ 3.7-001-99. Встановлює єдині вимоги до порядку створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу в комп’ютерних системах та захищених від несанкціонованого доступу компонентів обчислювальних систем.

Висновки. Діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути зосереджена на конструктивному поєднанні діяльності захист інформації (зокрема, забезпечення конфіденційності, цілісності та доступності інформації, у тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак). Важливе місце у вирішенні проблеми забезпечення інформаційної безпеки займає реалізація системи комплексного захисту інформації, котра є поєднанням у єдине ціле окремих елементів, механізмів, процесів, явищ, заходів, засобів і програм захисту інформації, взаємозв’язок яких сприяє реалізації цілей, концептуального підходу до питань функціонування і структурної побудови системи інформаційного забезпечення охорони і захисту.

Забезпечити абсолютну безпеку комп’ютерної інформації в телекомунікаційній мережі неможливо, так як абсолютно захищена система непридатна для її використання, крім того не всі шляхи подолання безпеки реально відомі.

Список використаних джерел:

1. Г. Почепцов, С. Чукут. Інформаційна політика: навч. посіб. К.: Знання,

2008. 663 с.

2. С.Е. Остапов, С.П. Євсеєв, О.Г. Король. Технології захисту інформації: навч. посіб. Х.: ХНЕУ, 2013. 476 с.

3. Ліпкан В.А. Теорія національної безпеки: підручник. К. : КНТ, 2009. 576 с. URL : http://politics.ellib.org.ua/pages-cat-154.html

4. Norbert Wiener. Cybernetics: Or Control and Communication in the Animal and the Machine. 2nd revised ed.. — Paris: Hermann & Cie, Camb. Mass. (MIT Press), 1961.

5. Глобальна та національна безпека: підручник / авт. кол. : В.І. Абрамов, Г.П. Ситник, В.Ф. Смолянюк та ін. Київ : НАДУ, 2016. 784 с.

6. Основи інформаційного права України : навч. посіб. / В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін; за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. К : Знання, 2004. 274 с.

7. Щиголь, Ю.Ф. Окремі аспекти державної політики України у сфері захисту інформації як об’єкта адміністративно-правового регулювання. Юридична наука, (3(105), 312–324. URL: https://doi.org/10.32844/2222-5374-2020-105-3.39

8. Засоби ТЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації. URL: https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi

Referances:

1. G. Pochepcov, S. Chukut. Informacijna polityka: navch. posib. K. : Znannja, 2008. 663 s. Print.

2. S.E. Ostapov, S.P. Jevsejev, O.G. Korol'. Tehnologii' zahystu informacii': navch. posib. H.: HNEU, 2013. 476 s. Print.

3. Lipkan V.A. Teorija nacional'noi' bezpeky: pidruchnyk. K. : KNT, 2009. 576 s. URL : http://politics.ellib.org.ua/pages-cat-154.html

4. Norbert Wiener. Cybernetics: Or Control and Communication in the Animal and the Machine. 2nd revised ed.. Paris : Hermann & Cie, Camb. Mass. (MIT Press), 1961. Print.

5. Global'na ta nacional'na bezpeka: pidruchnyk / avt. kol. : V.I. Abramov, G.P.Sytnyk, V.F. Smoljanjuk ta in. / za zag. red. G.P.Sytnyka. Kyi'v : NADU, 2016. 784 s.

6. Osnovy informacijnogo prava Ukrai'ny : navch. posib. / V.S. Cymbaljuk, V.D. Gavlovs'kyj, V.V. Grycenko ta in; za red. M.Ja. Shvecja, R.A. Kaljuzhnogo ta P.V. Mel'nyka. K : Znannja, 2004. 274 s. Print.

7. Shhygol', Ju.F. Okremi aspekty derzhavnoi' polityky Ukrai'ny u sferi zahystu informacii' jak ob’jekta administratyvno-pravovogo reguljuvannja. Jurydychna nauka, (3(105), 312–324. URL : https://doi.org/10.32844/2222-5374-2020-105-3.39

8. Zasoby TZI, jaki majut' ekspertnyj vysnovok pro vidpovidnist' do vymog tehnichnogo zahystu informacii'. URL : https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi.