УДК 355.6:658.7:351.74/.76

К. О. Споришев,
к. т. н., доцент, докторант ад'юнктури та докторантури,
Національна академія Національної гвардії України
ORCID ID: https://orcid.org/0000-0003-4737-9698

DOI: 10.32702/2306-6814.2024.4.224

ПІДСИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ СИЛАМИ БЕЗПЕКИ УКРАЇНИ

K. Sporyshev,
PhD in Technical Sciences, Associate Professor, Doctoral student of Adjunct
and Doctoral Studies, National Academy of the National Guard of Ukraine, Kharkiv, Ukraine

INFORMATION PROTECTION SUBSYSTEMS IN THE STATE MANAGEMENT SYSTEM OF THE SECURITY FORCES OF UKRAINE

Система державного управління силами безпеки України включає різноманітні підсистеми захисту інформації, оскільки забезпечення безпеки інформації є однією з найважливіших складових сучасної національної безпеки.

На сьогоднішній день до проблемних питань підсистеми захисту інформації в системі державного управління силами безпеки України можна віднести: несформованість чинного нормативно-правового поля; відсутність єдиного підходу до захисту інформації в системі державного управління силами безпеки України; поява новітніх викликів щодо захисту інформації; широке впровадження західних програмних продуктів та використання матеріально-технічної бази іноземного виробництва.

Проблема захисту інформації є комплексною і містить у собі як теоретичні й методологічні аспекти, так і технологію проектування та створення захищених систем і засобів захисту.

Об'єктами кіберзахисту є: комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Сучасні системи управління, які побудовані на базі обчислювальних мереж найбільш потребують встановлення та розробки новітніх систем захисту інформації. Найбільшою цінністю сучасності стає інформація.

В кожному суб'єкті сил безпеки має місце своя підсистема захисту інформації та вимоги до її захищеності. Ці фактори знижують ефективність державного управління підсистемами захисту інформації. Сили безпеки України є основним суб'єктом державної безпеки, тому захищеність інформації, що циркулює в мережах сил безпеки напряму впливає на державну безпеку. Витоки закритої інформації може призвести не тільки до іміджевих втрат держави, а і до втрат на полі бою.

Розробки та вдосконалення механізмів державного управління системами захисту інформації сил безпеки України вимагають виклики з якими зіткнулась наша держава. Під час збройної агресії рф проти України виникли нові загрози інформаційній безпеці, які потребують негайної реакції з боку сил безпеки та оборони.

The state management system of the security forces of Ukraine includes various subsystems of information protection, since information security is one of the most important components of modern national security.

To date, the problematic issues of the subsystem of information protection in the system of state management of the security forces of Ukraine include: the lack of formation of the current regulatory and legal field; lack of a unified approach to information protection in the state management system of the security forces of Ukraine; emergence of the latest challenges regarding information protection; wide implementation of Western software products and use of material and technical base of foreign production.

The problem of information protection is complex and includes both theoretical and methodological aspects, as well as the technology of designing and creating protected systems and means of protection.

The objects of cyber protection are: communication systems of all forms of ownership, in which national information resources are processed and/or which are used in the interests of state authorities, local self-government bodies, law enforcement agencies and military formations formed in accordance with the law; objects of critical information infrastructure; communication systems used to meet public needs and/or implement legal relations in the fields of electronic government, electronic public services, electronic commerce, and electronic document management.

Modern management systems, which are built on the basis of computer networks, most require the installation and development of the latest information protection systems. The greatest value of modernity is information.

Each subject of the security forces has its own subsystem of information protection and requirements for its security. These factors reduce the effectiveness of state management of information protection subsystems. The security forces of Ukraine are the main subject of state security, therefore the security of information circulating in the networks of the security forces directly affects state security. Leaks of classified information can lead not only to image losses of the state, but also to losses on the battlefield.

Development and improvement of mechanisms of state management of information protection systems of security forces of Ukraine require challenges faced by our state. During the armed aggression of the Russian Federation against Ukraine, new threats to information security arose, which require an immediate response from the security and defense forces.

Ключові слова: сили безпеки, підсистеми захисту інформації, державне управління, сучасні виклики державній безпеці.

Key words: security forces, subsystems of information protection, state administration, modern challenges to state security.

ПОСТАНОВКА ПРОБЛЕМИ

Система державного управління силами безпеки України включає різноманітні підсистеми захисту інформації, оскільки забезпечення безпеки інформації є однією з найважливіших складових сучасної національної безпеки. До основних підсистем захисту інформації в системі державного управління силами безпеки України відносяться:

Інформаційно-аналітична підсистема. Ця підсистема відповідає за збір, обробку, аналіз та використання інформації для прийняття рішень в сфері національної безпеки. Вона також включає в себе системи зберігання і захисту конфіденційної інформації.

Інформаційно-технічна підсистема. Ця підсистема включає в себе різноманітні технічні засоби захисту інформації, такі як системи шифрування, мережеві за-

ходи безпеки, антивірусні програми та інші засоби технічного захисту.

Інформаційно-правова підсистема. Забезпечує розвиток та впровадження правових актів, які регулюють сферу захисту інформації в державі. Це може включати законодавство про кібербезпеку, правила щодо обробки конфіденційної інформації, відповідальність за порушення правил захисту інформації тощо.

Організаційно-методична підсистема. Ця підсистема включає розробку та впровадження методик, стандартів, інструкцій та інших документів, які регулюють організаційні аспекти захисту інформації, включаючи процедури аудиту безпеки, навчання персоналу тощо.

Технологічна підсистема захисту інформації. Ця підсистема відповідає за впровадження сучасних технологій захисту інформації, таких як системи ідентифікації та аутентифікації, системи контролю доступу, механізми виявлення та реагування на кіберзагрози.

Ці підсистеми спільно працюють для забезпечення цілісності, конфіденційності та доступності інформації в системі державного управління силами безпеки України.

Перелічені підсистеми захисту інформації в системі державного управління силами безпеки України частково присутні у підсистемах захисту інформації в кожному з суб'єктів сил безпеки.

На сьогоднішній день до проблемних питань підсистеми захисту інформації в системі державного управління силами безпеки України можна віднести:

— несформованість чинного нормативно-правового поля;

— відсутність єдиного підходу до захисту інформації в системі державного управління силами безпеки України;

— поява новітніх викликів щодо захисту інформації;

— широке впровадження західних програмних продуктів та використання матеріально-технічної бази іноземного виробництва.

Проблема захисту інформації є комплексною і містить у собі як теоретичні й методологічні аспекти, так і технологію проектування та створення захищених систем і засобів захисту.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Значний внесок у дослідження проблемних питань захисту інформації в системах управління суб'єктів сил безпеки та оборони України зробили такі вчені як: Мацько О. Й., Микусь С. А., Солонніков В. Г., Дробаха Г. А., Олещенко О.А., Іохов О.Ю., Горелишев С.А., Сафошкіна Л.В., Лісіцин В. Е. ін. Питання забезпечення інформаційної безпеки держави розглянуті в працях вчених: Дудикевич В. Б., Опірський І. Р., Гаранюк П. І., Зачепило В. С., Партика А. І., Іванченко Є.В., Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є., Климчук О. О., Петрик В. М., Присяжнюк М. М., Мужанова Т.М..

МЕТА СТАТТІ

Метою статті є аналіз сучасного стану та існуючих проблем в підсистемах захисту інформації в системі державного управління силами безпеки України.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Згідно Закону України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 р. [1] під кібербезпекою розуміє 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].

Повноваження щодо протидії та запобігання основним видам загроз кібербезпеці: кіберзлочинності, кібераграсії та кібертероризму покладаються відповідно на правоохоронну сферу, сферу оборони і оборонно-промислового комплексу держави, сферу державної безпеки [1, 2].

Закон [1] визначає правові й організаційні засади забезпечення захисту національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, також повноваження та обов'язки державних органів в цієй сфері, основні принципи координації їх діяльності щодо забезпечення кібербезпеки.

Відповідно до Закону об'єктами кібербезпеки та кіберзахисту є [1]:

— конституційні права і свободи людини і громадянина;

— суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

— держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

— національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

— об'єкти критичної інфраструктури.

Об'єктами кіберзахисту, натомість, є: комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [1—4].

Важливим здобутком Закону України "Про основні засади забезпечення кібербезпеки України" є закріплення на законодавчому рівні базових понять у сфері кібербезпеки, а також визначення прав і обов'язків державних органів у цій сфері [2].

Відповідно до Закону 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 та-

кож заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури [1].

Повноваження щодо забезпечення безпеки в кіберпросторі має Президент України через очолювану ним Раду національної безпеки і оборони (РНБО); Національний координаційний центр кібербезпеки як робочий орган РНБО; Кабінет Міністрів і міністерства. Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів країни в кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України).

Основними суб'єктами національної системи кібербезпеки є [1—4]:

Держспецзв'язок та захист інформації, Національна поліція, СБУ, Міноборони та Генеральний штаб ЗСУ, розвідувальні органи, Національний банк України. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є: міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; ЗСУ, інші військові формування, утворені відповідно до закону; НБУ; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. Законом встановлено, що суб'єкти забезпечення кібербезпеки в межах своєї компетенції здійснюють низку різнопланових заходів [1—4]:

— заходи щодо запобігання використання кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

— виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

— інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

— розробку та реалізацію запобіжних, організаційних, освітніх та інших

заходів у сфері кібербезпеки, кібероборони та кіберзахисту;

— забезпечення проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

— інші заходи із забезпечення розвитку та безпеки кіберпростору.

Відповідно до Закону запропоновано такий розподіл функцій і повноважень органів державної влади у сфері кіберзахисту [1]:

Держспецзв'язку та захисту інформації здійснюватиме функції кіберзахисту об'єктів критичної інформаційної інфраструктури; координацію діяльності інших суб'єктів кібербезпеки; забезпечення створення та функціонування національної телекомунікаційної мережі; запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформування про кіберзагрози і методи захисту від них; забезпечення аудиту інформаційної безпеки на об'єктах критичної інфраструктури, установлення вимог до аудиторів інформаційної безпеки, визначення порядку їх атестації та переатестації;

На Національну поліцію (НПУ) покладено відповідальність за попередження, виявлення, припинення й розкриття кіберзлочинів;

Міністерство оборони та Генеральний штаб ЗСУ мають забезпечувати кібероборону військових об'єктів, кіберзахист об'єктів критичної інфраструктури під час війни і надзвичайного стану, а також відбивати військову агресію в кіберпросторі;

Служба безпеки України (СБУ) в межах своїх повноважень зобов'язана попереджати, виявляти, припиняти та розкривати злочини проти миру та безпеки людства в кіберпросторі, боротися з кібертероризмом і кібершпигунством, а також проводити таємні перевірки об'єктів критичної інфраструктури;

Національний банк є регулятором з кібербезпеки у банківській сфері і має право на встановлення власних стандартів в цій сфері і організацію перевірки їх дотримання. Завданням НБУ є також визначення порядку, вимог і заходів щодо забезпечення кіберзахисту та інформаційної безпеки в банківській системі, створення центру кіберзахисту та реєстру об'єктів критичної інформаційної інфраструктури в банківській системі.

Законом передбачено державно-приватну взаємодію у сфері кібербезпеки. Система своєчасного виявлення, попередження та нейтралізації кіберзагроз може бути створена із залученням волонтерських організацій. Передбачено підвищення цифрової грамотності громадян і культури безпеки поведінки в кіберпросторі. Заплановано обмін інформацією про кіберзагрози і координацію команд реагування на комп'ютерні надзвичайні події. Для громадян, представників промисловості та бізнесу створять консультаційні пункти. Крім того, буде створено систему підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки [1].

Отже, закладено нормативно-правові основи для розвитку національної системи забезпечення кібербезпеки України. Проведено розподіл повноважень між органами державної влади, визначено роль Національного координаційного центру кібербезпеки як суб'єкта, що координує та контролює діяльність суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку. Головним завданням є координація їх дій, процедур взаємодії та комплексних засобів реагування на загрози кібербезпеки держави, а також значна робота з запобігання кіберзлочинам [2].

Проте в Україні відсутні системні нормативні документи, які б детально описували загрози у кіберпросторі, надавали їх визначення та формували основи для цілісної державної політики з кібербезпеки. Додатко-

во, експерти відзначають недостатню кількість кадрів у сфері кібербезпеки у відомствах, що є наслідком низької якості підготовки та швидкого розвитку технологій, складнощів у залученні фахівців-практиків та небажання молодих спеціалістів працювати у державних структурах. Крім того, відсутні профільні науково-дослідні інститути, які б займалися комплексними дослідженнями з інформаційної та кібербезпеки.

За думкою деяких експертів, Україна залишається технологічно вразливою через широке використання західних програмних продуктів та матеріально-технічної бази іноземного виробництва. Шукати можливі "закладки" у цій продукції важко, але залежність від неї становить загрозливий рівень для національної безпеки. Проблема створення національної операційної системи залишається актуальною, а також відновлення вітчизняних потужностей у виробництві матеріально-технічної телекомунікаційної бази та створення національного антивірусу [2, 5].

Українське суспільство, включаючи державні органи, установи та особистості, має низьку культуру кібербезпеки та не усвідомлює необхідність дотримуватися вимог безпеки і наслідків, що можуть виникнути внаслідок їх неуважного ставлення до цього питання [2, 5].

ВИСНОВКИ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Сучасні системи управління, які побудовані на базі обчислювальних мереж найбільш потребують встановлення та розробки новітніх систем захисту інформації. Найбільшою цінністю сучасності стає інформація.

В кожному суб'єкті сил безпеки має місце своя підсистема захисту інформації та вимоги до її захищеності. Ці фактори знижують ефективність державного управління підсистемами захисту інформації. Сили безпеки України є основним суб'єктом державної безпеки, тому захищеність інформації, що циркулює в мережах сил безпеки напряму впливає на державну безпеку. Витоки закритої інформації може призвести не тільки до іміджевих втрат держави, а і до втрат на полі бою.

Розробки та вдосконалення механізмів державного управління системами захисту інформації сил безпеки України вимагають виклики з якими зіткнулась наша держава. Під час збройної агресії рф проти України виникли нові загрози інформаційній безпеці, які потребують негайної реакції з боку сил безпеки та оборони.

Література

1. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 р. https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Мужанова Т.М. Інформаційна безпека держави. Навчальний посібник — К.: ДУТ, ННІЗІ, 2019. — 131 с.

3. Забезпечення інформаційної безпеки держави: Навчальний посібник /В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с.

4. Климчук О. О. Забезпечення інформаційної безпеки держави :підручник / [О. О. Климчук, В. М. Петрик, М. М. Присяжнюк та ін.] ; за заг. ред. О. А. Семченка та В. М. Петрика. — К. : ДНУ "Книжкова палата України", 2015. — 672 с.

5. Основи інформатизації Національної гвардії України: навч. посіб. / Г. А. Дробаха, О. А. Олещенко, О.Ю. Іохов, В. Е. Лісіцин та ін. — Х. : НАНГ України, КП "Міська друкарня", 2016. — 366 с.

References:

1. The Verkhovna Rada of Ukraine (2017), The Law of Ukraine " About the main principles of ensuring cyber security of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Accessed 05 February 2024).

2. Muzhanova, T.M. (2019), Informatsiina bezpeka derzhavy [State information security], DUT, NNIZI, Kyiv, Ukraine.

3. Dudykevych, V. B. Opirskyi, I. R. Haraniuk, P. I. Zachepylo, V. S. and Partyka, A. I. (2017), Zabezpechennia informatsiinoi bezpeky derzhavy [Ensuring information security of the state], Vydavnytstvo Lvivskoi politekhniky, Lviv, Ukraine.

4. Klymchuk, O. O. Petryk, V. M. and Prysiazhniuk, M. M. (2015), Zabezpechennia informatsiinoi bezpeky derzhavy [Ensuring information security of the state], DNU Knyzhkova palata Ukrainy, Kyiv, Ukraine.

5. Drobakha, H. A. Oleshchenko, O. A. Iokhov, O.Iu. and Lisitsyn, V. E. (2016), Osnovy informatyzatsii Natsionalnoi hvardii Ukrainy [Basics of informatization of the National Guard of Ukraine], NANH Ukrainy, KP "Miska drukarnia", Kharkiv, Ukraine.

Стаття надійшла до редакції 09.02.2024 р.