УДК 316.776-049.5.65:351.862.4
DOI https://doi.org/10.32999/ksu2307-8049/2024-1-2

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В КОНТЕКСТІ СУЧАСНИХ ВИКЛИКІВ

Шевчук Михайло Олександрович,
кандидат юридичних наук,
докторант кафедри конституційного, адміністративного та фінансового права
Хмельницького університету управління та права
імені Леоніда Юзькова
m.shevchuk522@gmail.com
orcid.org/0000-0001-7549-6344

*Стаття має на **меті** аналіз системи управління інформаційною безпекою в Україні в контексті сучасних викликів, таких як кібератаки, шпигунство, поширення недостовірної інформації та втручання у внутрішні справи. Дослідження виконане на основі застосування низки **методів** наукового пізнання з використанням елементів діалектичного, нормативно-логічного, порівняльно-правового, формально-юридичного, системно-структурного та документального аналізу.*

***Результати.** Висвітлюючи важливість інформаційної безпеки для захисту суверенітету та територіальної цілісності країни, автор розглядає структурну організацію та функції різних органів управління інформаційною безпекою на національному рівні, включаючи Верховну Раду України, Президента України, Раду Національної безпеки і оборони, Кабінет Міністрів, а також регуляторні, контрольні та спеціалізовані органи, такі як Служба безпеки України та Державна служба спеціального зв'язку та захисту інформації. Стаття підкреслює комплексний підхід України до забезпечення інформаційної безпеки, що охоплює законодавче регулювання, стратегічне планування, міжвідомчу координацію та спеціалізовані заходи з протидії загрозам у кіберпросторі. У статті детально описано компетенції та основні завдання Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку), що відіграє центральну роль у забезпеченні інформаційної безпеки країни.*

***Висновки.** Отже, Україна розвиває комплексну та багаторівневу систему управління інформаційною безпекою, яка відповідає та протистоїть сучасним викликам, таким як кібератаки, шпигунство, дезінформація та втручання у внутрішні справи. Центральну роль у цій системі відіграє Державна служба спеціального зв'язку та захисту інформації, яка координує заходи з криптографічного та технічного захисту інформаційних ресурсів, забезпечуючи надійний зв'язок між органами державної влади та інтегрований захист інформаційних систем. Перспективи розвитку інформаційної безпеки в Україні пов'язані з поглибленням співпраці з міжнародними партнерами, обміном знаннями та технологіями, що дозволить ефективніше протистояти кіберзагрозам. З урахуванням динаміки розвитку кіберпростору система інформаційної безпеки має бути гнучкою та адаптивною, здатною оперативно реагувати на нові виклики та загрози.*

***Ключові слова:** інформаційна безпека, державне управління, органи управління, управління інформаційною безпекою, кібербезпека, кіберзагрози.*

INFORMATION SECURITY MANAGEMENT SYSTEM IN THE CONTEXT OF MODERN CHALLENGES

Shevchuk Mykhailo Oleksandrovych,
Candidate of Juridical Sciences,
Doctoral student at the Department of Constitutional, Administrative and Financial Law
Leonid Yuzkov Khmelnytskyi University of Management and Law
m.shevchuk522@gmail.com
orcid.org/0000-0001-7549-6344

*The **purpose** of this article is to analyze the information security management system in Ukraine in the context of modern challenges, such as cyber-attacks, espionage, dissemination of unreliable information and interference in internal affairs. The research is based on the application of a number of **methods** of scientific knowledge using elements of dialectical, normative-logical, comparative-legal, formal-legal, system-structural and documentary analysis.*

***The results.** Highlighting the importance of information security for the protection of the sovereignty and territorial integrity of the country, the author examines the structural organization and functions of various information security management bodies at the national level, including the Verkhovna Rada of Ukraine, the President of Ukraine, the National Security and Defense Council, the Cabinet of Ministers, as well as regulatory, control and specialized bodies, such as the Security Service of Ukraine and the State Service*

for Special Communications and Information Protection. The article emphasizes Ukraine's comprehensive approach to ensuring information security, which includes legislative regulation, strategic planning, interagency coordination and specialized measures to counter threats in cyberspace. The article describes in detail the competencies and main tasks of the State Service for Special Communications and Information Protection of Ukraine (State Special Communications), which plays a central role in ensuring the country's information security.

Conclusions. *Therefore, Ukraine is developing a comprehensive and multi-level information security management system that meets and resists modern challenges such as cyber-attacks, espionage, disinformation and interference in internal affairs. The central role in this system is played by the State Service for Special Communication and Information Protection, which coordinates measures for cryptographic and technical protection of information resources, ensuring reliable communication between state authorities and integrated protection of information systems. The prospects for the development of information security in Ukraine are related to the deepening of cooperation with international partners, the exchange of knowledge and technologies, which will allow more effective resistance to cyber threats. Taking into account the dynamics of cyberspace development, the information security system must be flexible and adaptive, capable of responding promptly to new challenges and threats.*

Key words: *information security, state administration, management bodies, information security management, cyber security, cyber threats.*

Вступ. В умовах сучасного інформаційного суспільства, де інформаційні технології проникають у всі сфери життя, забезпечення інформаційної безпеки стає пріоритетним завданням для держави. Ефективне управління інформаційною безпекою вимагає від державних органів не лише впровадження передових технологій, а й здатності адаптуватися до постійно змінюваних умов та загроз, особливо з огляду на посилений інтерес до інформаційної безпеки в умовах воєнного стану. Тому необхідно розглянути особливості функціонування державних органів у цей період. Значний внесок у розробку теоретичних основ державного управління інформаційною безпекою зробили українські дослідники, такі як В. Горбулін, О. Власюк, В. Горовенко, О. Дзьобань, Г. Ситник, М. Требін та інші.

Метою статті є аналіз інституційної структури та функцій органів державного управління у сфері інформаційної безпеки, а також визначення стратегій їх оптимізації з урахуванням сучасних викликів і загроз.

У сучасному світі, де інформація стала одним з ключових ресурсів розвитку держави та суспільства, питання інформаційної безпеки набуває особливої актуальності. Україна, як і більшість країн світу, стикається з різноманітними викликами в цій сфері – від кібератак та шпигунства до поширення недостовірної інформації та втручання у внутрішні справи.

Відповідно до Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу (Конституція України, 1996).

У Стратегії інформаційної безпеки дається визначення поняттю «інформаційна безпека України» як складової частини національної безпеки України, стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існування ефективної системи захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом (Стратегія інформаційної безпеки, 2022).

Реагуючи на ці виклики, Україна сформувала структурно повну систему органів управління інформаційною безпекою, кожен з яких відіграє важливу роль у забезпеченні захисту інформаційного простору країни.

1. Система органів управління інформаційною безпекою

Органи управління інформаційною безпекою загалом можна поділити на загальні, контрольні та спеціалізовані.

Загальними є органи управління на національному рівні. На найвищому рівні в ієрархії органів управління інформаційною безпекою перебувають Верховна Рада України та її спеціалізовані комітети, Президент України та Рада Національної безпеки і оборони України (РНБО). Верховна Рада через свої комітети відповідає за розробку законодавчих актів, що регулюють сферу інформаційної безпеки, тоді як Президент і РНБО координують діяльність усіх суб'єктів у цій сфері, визначаючи стратегічні напрями та пріоритети національної безпеки.

Кабінет Міністрів України через свої структури, зокрема Управління стратегії розвитку інформаційних ресурсів та технологій, втілює в життя державну політику в галузі інформаційної безпеки, забезпечуючи координацію та взаємодію між різними відомствами та організаціями.

Регуляторні та контрольні органи. Національна Рада України з питань телебачення та радіомовлення контролює дотримання законодавства у медіапросторі, забезпечуючи збалансованість та незалежність інформаційного простору. Генеральна прокуратура та судова система України забезпечують правовий захист у сфері інформаційної безпеки, розглядаючи справи, пов'язані з порушеннями у цій галузі.

Спеціалізовані органи. Серед спеціалізованих органів, які займаються питаннями інформаційної безпеки, особливе місце посідають Служба безпеки України (СБУ) та Державна служба спеціального зв'язку та захисту інформації України. Ці структури відповідають за забезпечення криптографічного захисту державної інформації, протидію кіберзлочинності та забезпечення захисту критичної інфраструктури.

Відповідно до п. 3 ч. 2 ст. 3 Закону України «Про основні засади забезпечення кібербезпеки України» Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки (Стратегія інформаційної безпеки, 2022). Крім цього, повноваження СБУ у сфері інформаційної безпеки визначені у спеціалізованому Законі «Про Службу безпеки України» (Про Службу безпеки України, 1992).

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) відіграє ключову роль у забезпеченні інформаційної безпеки країни. Утворена на основі Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» (Про Державну службу спеціального зв'язку та захисту інформації України, 2006), Держспецзв'язку є державним органом, що виконує комплекс завдань з розвитку, функціонування та захисту спеціальних телекомунікаційних систем.

Компетенція Держспецзв'язку:

1. Забезпечення урядового зв'язку: Держспецзв'язку розробляє та підтримує державні системи урядового та конфіденційного зв'язку, що забезпечують надійний зв'язок між вищими органами державної влади.

2. Реалізація державної політики у сфері захисту інформації: орган відповідає за розробку та впровадження заходів з криптографічного та технічного захисту інформації, а також захисту інформаційно-телекомунікаційних систем держави.

3. Комплексний захист інформаційних ресурсів: Держспецзв'язку забезпечує інтегрований захист інформаційних ресурсів, включаючи їх захист від несанкціонованого доступу, втручання чи знищення.

4. Контроль та нагляд: виконує функції контролю за станом безпеки спеціальних видів зв'язку та захисту інформації, забезпечуючи відповідність дій та заходів встановленим нормам і стандартам.

Таким чином, Держспецзв'язку виступає як центральний орган, який забезпечує захист інформаційного простору України, впроваджуючи комплексні заходи з криптографічного та технічного захисту інформації та зв'язку на державному рівні. Її діяльність є ключовою у забезпеченні національної безпеки та оборони держави в умовах сучасних інформаційних викликів і загроз.

2. Виклики та проблеми, з якими стикаються органи управління інформаційною безпекою

Органи управління інформаційною безпекою стикаються з низкою складних викликів та проблем, які вимагають комплексного підходу та постійного оновлення стратегій захисту. Одними з основних викликів є кіберзагрози та витоки інформації, що можуть мати різноманітні форми та масштаби. Поточні виклики у сфері інформаційної безпеки включають:

1. Кіберзагрози. Це охоплює широкий спектр атак, включаючи фішинг, віруси, трояни, шпигунське програмне забезпечення, DDoS-атаки тощо. Ці атаки можуть бути спрямовані на виведення з ладу інформаційно-комунікаційних систем, крадіжку конфіденційних даних або порушення нормальної роботи інформаційних систем.

2. Витік інформації. Несанкціонований доступ до конфіденційної інформації та її подальше поширення може призвести до значних фінансових збитків, втрати репутації та інших негативних наслідків для організацій та індивідів. Витоки можуть статися через слабкі місця в захисті даних, людські помилки або навмисні дії інсайдерів.

3. Застаріле та вразливе програмне забезпечення. Багато інцидентів безпеки починаються з експлуатації вразливостей у неоновленому або налаштованому за замовчанням програмному забезпеченні. Такі слабкі місця можуть бути легко використані зловмисниками для отримання несанкціонованого доступу до систем.

4. Недостатній контроль і моніторинг. Відсутність ефективних засобів контролю та моніторингу інформаційних потоків та діяльності в мережі може призвести до того, що атаки залишаються непоміченими до моменту, коли збиток стає значним.

Створена відповідно до Закону «Про основні засади забезпечення кібербезпеки України» Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA) активно працює над аналізом та нейтралізацією кіберзагроз, що становлять ризик для національної безпеки та інформаційного простору країни. Завданнями CERT-UA є: накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів; надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів; організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту; підготовка та розміщення на своєму офіційному вебсайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз; взаємодія з правоохоронними органами, забез-

печення їх своєчасного інформування про кібератаки; взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST зі сплатою щорічних членських внесків; взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору; опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту; сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам (Про основні засади забезпечення кібербезпеки України, 2017).

3. Заходи, спрямовані на підвищення рівня кіберзахисту в Україні

Реалізація низки заходів, спрямованих на підвищення рівня кіберзахисту в Україні, дала можливість досягти значних успіхів у протидії кібератакам. Досягнення та реалізовані заходи:

1. Проведення досліджень цільових атак: CERT-UA провела десятки детальних аналізів кібератак, що дозволило виявити основні вектори та методи атак зловмисників, а також розробити рекомендації для захисту від подібних загроз.

2. Ідентифікація вразливих систем: було визначено системи, доступні з мережі Інтернет, та складено перелік їх ідентифікаторів для подальшої перевірки та зміцнення їх захисту.

3. Використання сервісу shodan.io: застосування цього сервісу дозволило виявити асоційовані із системами вразливості та оперативно вжити заходів для їх усунення.

4. Ізоляція серверного обладнання: публічно доступні сервіси було ізольовано від локальних обчислювальних мереж та внутрішніх інформаційних систем для запобігання можливості горизонтального переміщення зловмисників у мережі в разі компрометації.

5. Обмеження доступу до інтерфейсів адміністрування: доступ до критичних сервісів адміністрування було обмежено, дозволяючи підключення лише з певних IP-адрес або через VPN, що суттєво підвищило рівень безпеки цих систем.

6. Впровадження багатофакторної автентифікації: реалізація додаткових рівнів перевірки під час авторизації у критичних системах значно знизила ризик несанкціонованого доступу.

7. Консультативна підтримка: CERT-UA надала консультативну допомогу організаціям у перевірці вебресурсів на наявність вразливостей, що допомогло вчасно ідентифікувати та усунути потенційні загрози.

Ці заходи разом з активним моніторингом та аналізом кіберзагроз дозволили знизити кількість успішних кібератак на 65%, навіть на тлі зростання активності хакерів (Завдання CERT-UA, 2024). Особлива увага приділялася захисту критичних об'єктів та інфраструктур, що мають стратегічне значення для національної безпеки.

Завдяки цим діям Україна продемонструвала високий рівень готовності та здатності до протидії сучасним кіберзагрозам, підтвердивши важливість комплексного підходу до кібербезпеки, що включає не лише технічні заходи, але й організаційні, правові та освітні ініціативи.

Однак існують й ускладнення, пов'язані з обмеженнями в компетенціях та ресурсах органів управління, такі як обмежені можливості впливу на приватний сектор, необхідність міжнародної співпраці та постійна еволюція кіберзагроз, що вимагає постійної адаптації стратегій захисту. Тому для ефективного вирішення проблем інформаційної безпеки потрібен комплексний підхід, що включає законодавчі ініціативи, технічні рішення, освітні програми та міжнародну співпрацю.

Досвід світової спільноти вказує на те, що ефективне вирішення питань захисту інформації, яка обертається у інформаційно-телекомунікаційних системах, та забезпечення надійного захисту цих систем від злочинних посягань, включаючи атаки з-за кордону, можливе тільки за умови створення комплексних систем захисту. Ці системи мають інтегрувати правові, організаційні, інженерні та технічні заходи разом із програмними засобами захисту.

У контексті міжнародного досвіду управління інформаційною безпекою система, розроблена та імплементована у Сполучених Штатах Америки, слугує яскравим прикладом комплексного та багаторівневого підходу. Відповідно до загальної політики та з урахуванням наявної базової інфраструктури та сформованої практики державного управління США створили й постійно вдосконалюють систему державних органів, відповідальних за інформаційну безпеку. Ключову роль у цій системі відіграє Комітет з національних систем безпеки (CNSS), який є одним з основних підрозділів у структурі президентської адміністрації США, спеціально створеним для вирішення завдань інформаційної безпеки. Цей комітет координує діяльність різних урядових агентств, забезпечуючи єдині стандарти та практики у сфері захисту національних інформаційних систем.

Загальна організаційна структура державного управління у сфері інформаційної безпеки у США характеризується високим рівнем складності та включає багато взаємопов'язаних елементів, які разом формують ефективну систему захисту інформаційного простору країни. Ця система постійно адаптується до змінюваних умов та нових викликів у галузі кібербезпеки, що дозволяє Сполученим Штатам ефективно протистояти різноманітним загрозам інформаційній безпеці.

Висновки. Україна розвиває комплексну та багаторівневу систему управління інформаційною безпекою, яка відповідає сучасним викликам, таким як кібератаки, шпигунство, дезінформація та втручання у внутрішні

справи. Центральну роль у цій системі відіграє Державна служба спеціального зв'язку та захисту інформації, яка координує заходи з криптографічного та технічного захисту інформаційних ресурсів, забезпечуючи надійний зв'язок між органами державної влади та інтегрований захист інформаційних систем.

З огляду на глобальний характер інформаційних загроз важливо продовжувати вдосконалення законодавчого регулювання, стратегічного планування та міжвідомчої координації. Особливу увагу слід звернути на модернізацію технічної інфраструктури, підвищення рівня професійної підготовки фахівців у галузі кібербезпеки та залучення міжнародного досвіду.

Перспективи розвитку інформаційної безпеки в Україні пов'язані з поглибленням співпраці з міжнародними партнерами, обміном знаннями та технологіями, що дозволить ефективніше протистояти кіберзагрозам. З огляду на динаміку розвитку кіберпростору система інформаційної безпеки має бути гнучкою та адаптивною, здатною оперативно реагувати на нові виклики та загрози.

Завдяки комплексному підходу, активній ролі спеціалізованих органів, таких як Держспецзв'язку та CERT-UA, а також застосуванню передового міжнародного досвіду Україна має всі можливості для зміцнення своєї інформаційної безпеки та захисту критичної інфраструктури від сучасних кіберзагроз.

ЛІТЕРАТУРА:

1. Конституція України від 28.06.1996. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/conv#Text (дата звернення: 16.02.2024).

2. Стратегія інформаційної безпеки. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14 (дата звернення: 20.04.2022).

3. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12/conv#top (дата звернення: 16.02.2024).

4. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 16.02.2024).

5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 16.02.2024).

6. Завдання CERT-UA. URL: https://cert.gov.ua/about-us (дата звернення: 16.02.2024).

REFERENCES:

1. Constitution of Ukraine. (1996, June 28). Verkhovna Rada of Ukraine. Retrieved February 16, 2024 from: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/conv#Text.

2. Information Security Strategy. (2021). Verkhovna Rada of Ukraine. Retrieved April 20, 2022 from: https://zakon.rada.gov.ua/laws/show/685/2021#n14.

3. On the Security Service of Ukraine: Law of Ukraine No. 2229-XII. (1992, March 25). Verkhovna Rada of Ukraine. Retrieved February 16, 2024 from: https://zakon.rada.gov.ua/laws/show/2229-12/conv#top.

4. On the State Special Communications Service and Information Protection of Ukraine: Law of Ukraine No. 3475-IV. (2006, February 23). Verkhovna Rada of Ukraine. Retrieved February 16, 2024 from: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

5. On the Basic Principles of Cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII. (2017, October 5). Verkhovna Rada of Ukraine.

6. Tasks of CERT-UA. CERT-UA. Retrieved February 16, 2024 from: https://cert.gov.ua/about-us.

Стаття надійшла до редакції 28.02.2024
The article was received 28 February 2024