ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЯК СКЛАДОВОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ[1]

ДУМЧИКОВ Михайло Олександрович - кандидат юридичних наук, старший викладач кафедри кримінально-правових дисциплін та судочинства Навчально-наукового інституту права Сумського державного університету

ORCID: https://orcid.org/0000-0002-4244-2419,
e-mail: m.dumchykov@yur.sumdu.edu.ua

УДК 342.841
DOI 10.32782/LAW.UA.2023.3.32

У цій статті проведено аналіз актуальних проблем у сфері забезпечення кібербезпеки, які стають ключовими в сучасних реаліях державності із розвинутою інформаційною інфраструктурою та численними вразливими об'єктами. Висвітлено існуючі загрози для кібербезпеки та проблеми, пов'язані з ефективністю заходів забезпечення національної безпеки системи кіберзахисту. Стаття розкриває особливості вразливості сучасних інформаційно-телекомунікаційних систем і критично важливої інфраструктури.

Проаналізовано поточний стан забезпечення кібербезпеки в Україні, зосереджено увагу на основних аспектах нормативно-правового забезпечення інформаційної безпеки країни. Виявлено основні оголошені заходи протидії загрозам інформаційній безпеці загалом і за окремими її аспектами. Відзначено відсутність практичного виконання цих заходів. Визначено ключові проблеми в забезпеченні кібербезпеки, такі як неефективність нормативно-правової бази та системи управління; відсутність єдиної стратегії кіберзахисту; недостатній рівень державного управління у сфері кіберзахисту; відсутність трансформаційного підходу до управління національною кібербезпекою від держави; розмитість вимог до систем захисту інформації; використання застарілих стандартів.

Автор підкреслює необхідність спільних зусиль міжнародного співтовариства у вирішенні проблем кібербезпеки. Особлива увага приділяється заходам захисту систем, мереж та програмних додатків від цифрових атак, а також важливості прийняття нових міжнародних законів, спрямованих на підвищення рівня кібербезпеки.

Ключові слова: інформаційна безпека, критична інфраструктура, цифровізація, кібербезпека, кібератаки, кіберзлочинність, безпека у кіберпросторі.

Постановка проблеми

Розвиток інформаційно-телекомунікаційних технологій та настанням епохи інформаційного суспільства стають каталізаторами викликів у сфері забезпечення кібербезпеки, що вимагає новаторських підходів та рішень.

Шлях України у забезпеченні дійсно діючої системи кібербезпеки потребує радикальних та невідкладних змін. При чому, така вимога випливає не лише з трансформацією цифрового суспільства та особистості, а перш за все з численністю атак на об'єкти критичної інформаційної інфраструктури держави. Варто зауважити, що сьогодні Україна виступає кібрполігоном у веденні кібервійни.

Ми переконані, що безпека інформаційного простору та його складової частини – кіберпростору, гарантування безпеки й сталого функціонування національної критичної інфраструктури, інформаційно-телеко-

[1] «Виконання завдань перспективного плану розвитку наукового напряму «Суспільні науки» Сумського державного університету» (номер державної реєстрації БФ/24-2021, термін виконання 2021-2025 роки).

мунікаційних систем повинна стати не лише складовою державної політики у сфері розвитку кібернетичного простору та становлення цифрової особистості, а й включення перелічених чинників у сферу політичних та стратегічних напрямків держави.

Стан дослідження проблеми

Питанням щодо проблеми забезпечення кібербезпеки, як складової інформаційної безпеки та внесення вагомого внеску у розв'язання згаданих проблем на теоретичному рівні зробили такі науковці, як В. Л. Бурячок, В. В. Кравчук, М. В. Гуцалюк,, В. В. Кравчук, О. Д. Довганя, В. С. Серьогіна. Водночас, проблематика забезпечення кібербезпеки в умовах збройної агресії Російської Федерації залишається актуальною проблемою.

Мета і завдання дослідження

Метою статті є дослідження проблематики забезпечення кібербезпеки, як складового елемента інформаційної безпеки держави у сучасних умовах, визначення основних кіберзагроз та вироблення дієвого механізму їх нівелювання.

Виклад основного матеріалу

Швидкий розвиток інформаційно-телекомунікаційних технологій та їх широке впровадження в цифрове суспільство стало каталізатором зростання рівня кіберзагроз. Згідно з доповіддю IBM «X-Force Incident Response and Intelligence Services», кількість кібератак, спрямованих на крадіжку даних та заподіяння шкоди критичній інфраструктурі, потроїлася у першій половині 2022 року. За прогнозами Центру кібербезпеки Всесвітнього економічного форуму, у 2023 році 74% всіх глобальних компаній стануть жертвами кібернетичних атак [1].

Кібербезпека сьогодні є однією з найважливіших тем у сучасному світі. Проте важливо розрізняти поняття кібербезпеки та інформаційної безпеки, що наразі спричинює плутанину серед великої кількості людей.

Таким чином кібербезпека становить лише частину загального обсягу інформаційної безпеки, обмежуючись електронними аспектами інформаційного простору, зокрема через низьку аспектів: 1) фокус на цифрових технологіях (кібербезпека концентрується на захисті виключно цифрової інформації яка обертається в інформаційно-телекоунікаційних системах, включає в себе заходи безпеки, спрямовані на мережі, комп'ютери, програми та інші аспекти цифрового середовища; 2) інформаційно-телекомунікаційна орієнтованість (кібербезпека зазвичай стосується захис-

Таблиця № 1. Співвідношення сутності понять кібербезпека та інформаційна безпека.

Критерій	Інформаційна безпека	Кібербезпека
Визначення	Захист інформації взагалі, незалежно від форми та типу.	Фокус на захисті інформації в мережі та цифровому середовищі.
Сфера застосування	Включає всі аспекти захисту інформації у фізичній та цифровій формах.	Спрямована на захист виключно цифрової інформації та комп'ютерних систем.
Об'єкти захисту	Фізичні та електронні носії інформації, документи, приміщення тощо.	Комп'ютерні системи, мережі, програми та цифрові дані.
Загрози	Можуть бути фізичними або електронними, внутрішніми або зовнішніми.	Головним чином електронні загрози, такі як хакерські атаки, віруси тощо.
Заходи безпеки	Фізичний контроль доступу, політики, процедури та технічні заходи.	Антивірусне програмне забезпечення, мережеві заходи, криптографія тощо.
Обсяг	Ширший спектр, охоплює всі аспекти, пов'язані з інформацією.	Специфічно спрямований на область цифрових технологій та комп'ютерів.

ту комп'ютерних систем, мереж і данних, орієнтована на виявлення, запобігання та врегулювання цифрових загроз, таких як хакерські атаки, віруси, шкідливий програмний код тощо; 3) цифрові загрози (основними загрозами для кібербезпеки є електронні атаки, які виникають в кібернетичному середовищі [2].

Саме це відрізняє кібербезпеку від інформаційної безпеки, яка може включати загрози фізичного характеру або інші форми неприязної діяльності. Водночас, сьогодні саме забезпечення кібербезпеки є нагальною та актуальною потребою держави, враховуючи ті виклики, з якими вона стикається сьогодні: 1) зростання кількості кіберзагроз; 2) цифрова трансформація держави та залежність від інформаційно-телекомунікаційних технологій; 3) збільшення розміру та складності телекомунікаційних мереж; 4) збільшення обсягу цінності цифрових даних, які обертаються в інформаційно-телекомунікаційних мережах; 5) глобальний характер кіберзагроз [3, с. 155].

Кібербезпека спрямована на виявлення та відбиття загроз в кібернетичному просторі, щодо об'єктів, пов'язаних із ІТ-технологіями, комп'ютерами, телекомунікаційними мережами, а також зберіганням, обробкою та передачею цифрової інформації. Водночас, відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [4].

У сучасному світі забезпечення кібернетичної безпеки виступає не локальною проблемою окремих суб'єктів, а глобальною проблемою. Сьогодні мета кібератак настільки обширна, що вже виходить за межі окремих хакерських атак та кримінальних правопорушень економічного характеру, сьогодні такою метою виступає рівень безпеки державної критичної інфраструктури. Інновації в галузі ІТ-технологій в сучасній Україні є ключовим фактором цих змін. Державні та транснаціональні компанії, а також окремі користувачі вже не уявляють свого життя без них, і все більше фінансових операцій здійснюється через Інтернет. Кіберзлочинці усвідомили, які величезні можливості для «заробітку» грошей виникли в останні часи, і багато з нинішніх шкідливих програм написані на замовлення або з метою подальшого продажу іншим злочинцям. У результаті злочинний ланцюг замикається у великому кільці організованої кіберзлочинності [5, с. 14].

Хочемо зупинитися на найнебезпечніших кіберзагрозах, об'єктом яких сьогодні все частіше стає наша держава. Першою загрозою, яку ми хочемо виділити – це кібератаки на об'єкти критичної інфраструктури.

Існує багато трактувань поняття «критична інфраструктура», зокрема у відображені національних, економічних, політичних чи культурних тенденцій, потреб та інтересів. Водночас, загальні риси усіх цих трактувань, включають в собі ідею про те, що інфраструктури у загальному вигляді є засобами загального призначення для різних видів людської діяльності. Загальні риси всіх цих визначень включають зокрема економічної діяльності, але також і для дій, необхідних для захисту безпеки та здоров'я громадян. Варто зауважити, що сьогодні всі системи, які входять до критичної інфраструктури, засновані інформаційно-телекомунікаційних технологіях і є неоднаково чутливими до кібератак. Наприклад, лікарні та телекомунікаційні системи, енергетика, банківська та фінансовий сектори, а також поштовий сектор – усі вони у тій чи іншій мірі покладаються на кіберінфраструктуру,

що робить їх очевидними цілями для кіберзлочинців.

Кібератаки на об'єкти критичної інфраструктури сьогодні можна порівняти з тероризмом в кібернетичному просторі. Наслідками таких атак, можуть буди втрата стратегічної інформації, викрадення даних клієнтів банківських установ, відключення електропостачання на підприємствах, установах, організація, тощо.

Напевно, найпоширеніший вид кібератак на державну критичну інфраструктуру є DDoS атаки. DDos атаки представляють собою атаки на комп'ютерні системи органу, організації, установи з метою порушення доступності атакованих вебресурсів. Зазвичай DDoS-атаки здійснюють із метою поширення паніки та дестабілізації. Іноді використовують для приховування деструктивних дій, тобто коли DDoS-атака слугує прикриттям атаки іншого виду. Проте самі DDoS-атаки загрози для персональних даних громадян не становлять. Варто знати, що для проведення DDoS-атак хакери часто використовують зламані пристрої людей. Тому важливо дотримуватися основних правил кібергігієни, користуватися антивірусами, оновлювати вчасно програмне забезпечення тощо [6].

Водночас, на спільному брифінгу Мінцифри, РНБО, НКЦК, Держспецзв'язку, СБУ, НБУ та Кіберполіції було повідомлено, що 15 лютого Україна відбила найбільшу в історії країни DDoS-атаку, що була спрямована на банківський сектор, офіційні сайти органів влади, енергетичний блок та портал Дія [7].

Загроза кібератак на інфраструктуру держави здатна мотивувати її до розширення кібер-можливостей. На жаль, деякі контрзаходи з боку держави не ведуть до безпосереднього посилення кіберзахисту країни, а скоріше сприяють слідчим можливостям. Посадові особи держави можуть визнати, що існують структурні обмеження, які перешкоджають покращенню кіберзахисту деяких критично важливих інфраструктур ступеня, необхідного для цілей національної безпеки. Зазначимо, що ці обмеження зумовлені існуючою мережею інформаційно-телекомунікаційних систем управління, яка є «унікальним середовищем, що поєднує великомасштабні, географічно розподілені, застарілі та власні компоненти системи» [8].

Варто зауважити, що об'єктом кібератак стають не лише державні інфраструктурні об'єкти, але й звичайні люди. Пропорційно підвищенню кількості кібератак на державний сектор, збільшилися і кібератаки на громадян України. За даними Департаменту кіберполіції Національної поліції України за 2022 рік було зареєстровано близько 2 300 тис. справ в ЄРДР, та повідомлено про підозру близько 1 000 тис. осіб. Водночас, поступило близько 62 000 тис. звернень громадян про їх порушені права та свободи в рамках кіберпростору [9].

Згідно даних Державної служби спеціального зв'язку та захисту інформаційні, лише за перший квартал 2023 року було зареєстровано 762 кіберінцедентів об'єктом яких виступала критична інфраструктура держави. Зазначається, що в другому півріччі 2022 року було зареєстровано 342 кібератаки, у середньому 57 зареєстрованих інцидентів на місяць та 1-2 на добу. При цьому за 6 місяців у першому півріччі 2023 року зареєстрованих кібератак вже було 762, у середньому 128 на місяць та 4-5 на добу [10].

Стратегічні пріоритети України та багатьох інших країн спрямовані на захист критично важливої інфраструктури, яка може зіткнутися з низкою загроз, у тому числі кіберзагрозами.

Враховуючи широке використання інформаційно-телекомунікаційних технологій у різних промислових та економічних галузях, розробка систем та підходів у галузі кібербезпеки є однієї з пріоритетних областей та потребує постійного вдосконалення з урахуванням постійної появи нових типів кіберзагрози. У зв'язку з цим важливим аспектом створених рішень є оновлення інформації про існуючі типи кіберзагроз, а також інформацію про їх усунення та підтримку поточного ступеня кіберзахисту внутрішньої інфраструктури. Проблема кібербезпеки відіграє ключову роль, оскільки внутрішня інформаційна інфраструктура містить величезну кількість структурованих та неструктурованих даних, яким потрібні величезні ресурси для захисту об'єктів від кіберзагроз.

Література

1. 2022 Norton cybercrime report, a worrying scenario. Security Affairs. Офіційний веб-ресурс. URL: https://securityaffairs.com/
2. Emmanuel Salami's Lab. Enhancing global security and peaceful coexistence: the imperatives ofcyberseurity architecture. URL: https://www.researchgate.net/publication/368636312_ENHANCING_GLOBAL_SECURITY_AND_PEACEFUL_COEXISTENCE_THE_IMPERATIVES_OF_CYBERSEURITY_ARCHITECTURE_1
3. Трофименко О.С. Кібербезпека України: аналіз сучасного стану. Захист інформаціїю. 2019. Том 21. № 3. С. 150-158.
4. Закон України: Про основні засади забезпечення кібербезпеки України № 2163-VIII від 05.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Безуглий Д.Ю. Інформаційна безпека України: огляд останніх тенденцій. Фізико-математична освіта. 2018. вип. 2(16). С. 13–17.
6. Що таке DDoS-атака?. Державна служба спеціального зв'язку та захисту інформації України. Офіційний веб-ресурс. URL: https://cip.gov.ua/ua/faqs/sho-take-ddos-ataka
7. Україна успішно відбила найбільшу DDoS-атаку в своїй історії. Державна служба спеціального зв'язку та захисту інформації України. Офіційний веб-ресурс. URL: https://cip.gov.ua/ua/news/ukrayina-uspishno-vidbila-naibilshu-ddos-ataku-v-svoyii-istoriyi
8. Янковський О.А. Україні потрібна нова кіберстратегія. URL: https://www.pravda.com.ua/columns/2019/09/14/7226291/
9. Департамент Кіберполіції Національної поліції України. Офіційний веб-русурс. URL: https://cyberpolice.gov.ua/
10. Російські хакери у 2023 році збільшили кількість атак на Україну: що відомо. Інформаційне агенство УНІАН. Офіційний веб-ресурс. URL: https://www.unian.ua/war/rosiyski-hakeri-u-2023-roci-zbilshili-kilkist-atak-na-ukrajinu-shcho-vidomo-12426765.html

SUMMARY

This article analyzes current problems in the field of cyber security, which are becoming key in the modern realities of statehood with a developed information infrastructure and numerous vulnerable objects. The existing threats to cyber security and problems related to the effectiveness of measures to ensure the national security of the cyber defense system are highlighted. The article reveals the specifics of the vulnerability of modern information and telecommunication systems and critical infrastructure.

The current state of ensuring cyber security in Ukraine is analyzed, attention is focused on the main aspects of the regulatory and legal provision of information security in the country. The main declared countermeasures against threats to information security in general and by its individual aspects have been identified. The lack of practical implementation of these measures was noted. The key problems in ensuring cyber security are identified, such as the ineffectiveness of the legal framework and management system; lack of a unified cyber defense strategy; insufficient level of state management in the field of cyber protection; lack of a transformational approach to the management of national cyber security from the state; blurring of requirements for information protection systems; using outdated standards.

The author emphasizes the need for joint efforts of the international community in solving cyber security problems. Special attention is paid to measures to protect systems, networks and software applications from digital attacks, as well as the importance of adopting new international laws aimed at increasing the level of cyber security.

Keywords: information security, critical infrastructure, digitalization, cyber security, cyber attacks, cyber crime, security in cyber space.