Добровольська Тетяна Миколаївна,
здобувач ступеня вищої освіти магістра інституту заочного та дистанційного навчання Національної академії внутрішніх справ
Науковий керівник:
Шрамко С. С., завідувач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, старший дослідник

КІБЕРБЕЗПЕКА У ВОЄННИЙ ЧАС: НОВІ ТЕНДЕНЦІЇ ТА ПРАВОВІ АСПЕКТИ

Кібербезпека у воєнний час охоплює правові, організаційні, технічні й інформаційні механізми, спрямовані на захист цифрового простору держави. Вона включає діяльність спеціально уповноважених суб'єктів, наділених відповідними повноваженнями у сфері протидії кіберзагрозам, які використовують методи, засоби та технології для виявлення, запобігання й нейтралізації небезпечних впливів на інформаційні ресурси.

Кібербезпеку також можна розглядати як рівень захищеності національних інформаційних ресурсів від зовнішніх і внутрішніх загроз, зокрема кібератак, інформаційних диверсій та спроб несанкціонованого втручання у функціонування інформаційно-телекомунікаційних систем.

Цифровий простір став одним із ключових фронтів протистояння в умовах повномасштабної війни. Кібератаки, інформаційні диверсії та спроби несанкціонованого втручання у роботу державних і військових систем стали складовою гібридної агресії російської федерації. У зв'язку з цим забезпечення національної кібербезпеки є критично важливим елементом обороноздатності держави, а її правове, організаційне та технічне регулювання потребує постійного вдосконалення.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає поняття кіберзлочин або комп'ютерний злочин як суспільно-небезпечні дії, як умисні, так

і вчинені з необережності, що здійснюються у кіберпросторі або з його використанням; кримінальна відповідальність за такі діяння передбачена Кримінальним кодексом України [1]. Метою таких протиправних дій часто стає викрадення або знищення інформації, порушення роботи інформаційних систем чи мереж. Особливо в умовах війни кіберзлочинці спрямовують свої зусилля на дестабілізацію державних інститутів, на завдання шкоди інфраструктурі, порушення функціонування обладнання і доступу до секретних даних.

У згаданому законі говориться, що об'єктами атак виступають системи, від функціонування яких залежить стабільність держави: інформаційні ресурси органів державної влади, Збройних Сил України, правоохоронних органів, засобів масової інформації та інших структур, що здійснюють комунікацію між державою і суспільством [1].

До категорії критичних об'єктів також належать енергетичні та промислові підприємства, зокрема атомні електростанції та підприємства хімічної галузі. Їх інформаційно-комунікаційні системи віднесено до критичної інфраструктури про що йдеться у Законі України «Про критичну інфраструктуру», з огляду на потенційну небезпеку наслідків їх порушення для життя, здоров'я людей і національної безпеки держави [2]. Підвищена увага спрямована й до транспортних мереж, системи електронного урядування, електронної комерції та документообігу, які забезпечують безперервність функціонування державних послуг та економічних процесів. Важливою складовою є також фінансовий сектор — банківські установи, платіжні системи та інші сервіси, збої у роботі яких можуть викликати масштабні економічні ризики. Саме тому законодавець відносить такі структури до секторів критичної інфраструктури, які потребують особливого режиму захисту [3].

З початком повномасштабної воєнної агресії проти України суттєво зросла кількість кібератак, спрямованих як на державні, так і на приватні структури. Одним із прикладів стала спроба кібератаки, здійсненої хакерським угрупованням Strontium (APT28), яке намагалося проникнути в комп'ютерні мережі України, Сполучених Штатів Америки та країн Європейського Союзу. Метою було отримання тактичної інформації для підтримки військових дій росії та викрадення конфіденційних даних, що стосуються державних і безпекових структур [4].

Фахівці Державної служби спеціального зв'язку та захисту інформації України неодноразово фіксували нові спроби фішингових розсилок, відкриття яких давало можливість хакерам встановити шкідливе програмне забезпечення та отримати повний контроль над зараженими пристроями [5]. Схожі атаки були із застосуванням шкідливого програмного забезпечення Cobalt Strike Beacon, яке використовувалося російськими хакерами для ураження державних інформаційних систем було із спробою компрометації комп'ютерів державних органів через розсилку заражених документів [6].

Вважливим елементом кіберзахисту держави стала співпраця уряду та українського IT-сектору. Провідні компанії галузі об'єднали зусилля для протидії кібератакам, які спрямовуються проти об'єктів критичної інфраструктури, державних ресурсів та бізнесу. IT-фахівці здійснюють моніторинг, виявлення й нейтралізацію ворожих кіберзагроз, включно з діяльністю російських хакерських угруповань і бот-мереж, а також сприяють безперервному функціонуванню цифрових сервісів. Наприклад, компанія GigaCloud, яка під час активних бойових дій безкоштовно здійснила міграцію дата-центру Prozorro з Києва до Львова, забезпечивши збереження критичних даних та безперервність роботи державної електронної системи закупівель, попри ракетні обстріли [7].

З урахуванням зазначених інцидентів, кримінальна відповідальність за певні діяння, які пов'язані з кіберзлочинністю, була посилена. Стаття 361-1 Кримінального кодексу України, чітко передбачає відповідальність за створення або розповсюдження шкідливих програмних чи технічних засобів, що можуть бути використані для несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, мереж або мереж електрозв'язку [8].

Законодавцем розширено перелік кримінально караних дій у сфері несанкціонованого втручання в роботу комп'ютерних систем, а також передбачено більш суворі санкції у випадках, коли такі злочини завдають шкоди об'єктам критичної інфраструктури держави [9], та удосконалено процедури виявлення, документування та розслідування кіберзлочинів, що дозволяє правоохоронним органам оперативніше реагувати на кібератаки та підвищує ефективність притягнення винних до відповідальності [10].

Підсумовуючи викладене, зазначимо таке:

1. Зростання кількості ворожих кібератак, спроб проникнення хакерських угруповань у мережі державних установ і оборонних структур України, підтверджує реальність та масштабність кіберзагроз.

2. Сучасні воєнні конфлікти значною мірою виходять за межі традиційного бойового протистояння, саме тому захист держави у цифровій сфері стає рівнозначним із забезпеченням її обороноздатності.

3. В умовах воєнного стану кібербезпека постає як технічним та інформаційним питанням, так і складовою національної безпеки, без якої неможливе стабільне функціонування держави, її економіки та систем управління.

4. Актуалізується необхідність правового, організаційного та технологічного забезпечення стійкості держави перед зростаючими кіберзагрозами, що є невід'ємною частиною сучасних воєнних дій.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

3. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього : постанова Кабінету Міністрів України від 28.04.2023 № 415. URL: https://zakon.rada.gov.ua/laws/show/415-2023-п#Text

4. Яворович Т. Корпорація Microsoft запобігла спробам хакерів ГРУ атакувати українські інституції. *Суспільне новини*. URL: https://suspilne.media/226405-korporacia-microsoft-zapobigla-rosijskim-kiberatakam-na-ukrainski-organizacii.

5. Державна служба спеціального зв'язку та захисту інформації України. Хакери розсилають військовослужбовцям ЗСУ повідомлення зі шкідливим програмним забезпеченням під виглядом рекрутингу до 3 ОШБр та ЦАХАЛ. cip.gov.ua. URL: https://cip.gov.ua/ua/news/khakeri-rozsilayut-viiskovosluzhbovcyam-zsu-povidomlennya-zi-shkidlivim-programnim-zabezpechennyam-pid-viglyadom-rekrutingu-do-3-oshbr-ta-cakhal.

6. Veronika Telychko. Cobalt Strike Beacon Malware Detection: A New Cyber-Attack on Ukrainian Government Organizations Attributed to the UAC-0056 Group. socprime.com. URL: https://socprime.com/blog/cobalt-strike-beacon-malware-detection-a-new-cyber-attack-on-ukrainian-government-organizations-attributed-to-the-uac-0056-group/?utm_source=chatgpt.com.

7. Lviv It Cluster. Хмарний оператор GigaCloud запустив оновлений дата-центр у Львові. Чому це важливо для бізнесу під час війни. itcluster.lviv.ua. URL: https://itcluster.lviv.ua/hmarnyj-operator-gigacloud-zapustyv-onovleny.

8. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 17 лип. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

9. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text

10. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text