Бейкун А. Л.,
кандидат юридичних наук, доцент,
доцент кафедри правового забезпечення
та правоохоронної діяльності
факультету забезпечення державної безпеки
Київського інституту Національної гвардії України
(м. Київ, Україна)

Бойчук В. В.,
здобувач вищої освіти
факультету службово-бойової діяльності НГУ
Київського інституту Національної гвардії України
(м. Київ, Україна)

ІНФОРМАЦІЙНА СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ КРИТИЧНИХ ЗАГРОЗ ДЕРЖАВНОСТІ: ПРАВОВІ ТА ПОЛІТИЧНІ АСПЕКТИ

Інформаційна та кібернетична безпека займає особливе місце в загальній системі національної безпеки держави, оскільки є елементом усіх складових системи безпеки, внаслідок чого одночасно набуває й самодостатнього значення. Будь-які виклики чи загрози власне національній безпеці країни безпосередньо стосуються також її інформаційної складової [1].

Вирішення питань інформаційної та кібернетичної безпеки, насамперед, пов'язане із необхідністю захисту національного інформаційного простору та розвитку інформаційно-комунікаційної системи для забезпечення державної інформаційної політики, у тому числі, в умовах ескалації зовнішніх загроз та небезпек для держави до критичного рівня.

Наприкінці третього року від початку повномасштабної збройної агресії, російська федерація залишається основним джерелом загроз національній та міжнародній кібербезпеці, яка активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у війні проти України. Така деструктивна активність створює реальну загрозу реалізації наявних можливостей відбиття актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури.

Ще задовго до повномасштабного вторгнення росія посилила кібератаки на державні органи, оборонно-промисловий комплекс, інфраструктурні об'єкти, ІТ-мережі та ЗМІ в Україні. Кіберборотьба й кіберзахист стали одними із ключових елементів війни. Наші фахівці та хакери-волонтери не лише успішно протистоять нападам, а й завдають дошкульних ударів у відповідь. Торік зафіксовано понад 1,25 мільйона DDoS-атак на російську інфраструктуру (це 8,4% від усіх кібератак у світі). За оцінками керівника служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО, Україна – єдина держава,

яка змогла здобути перевагу у протистоянні кібератакам та інформаційній агресії російської федерації. Проте маємо усвідомлювати: про остаточну перемогу наразі не йдеться. Ворог удосконалюється, маневрує, змінює вістря ударів. Нинішній тренд - інтелектуальні атаки задля виявлення слабких місць в інфраструктурі. І світовий досвід доводить: надійна робота систем кіберзахисту залишатиметься актуальною і в мирний час [2].

Кіберпростір разом з іншими фізичними просторами де-юре визнано і фактично є одним з театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту національної критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами.

У зв'язку з триваючою повномасштабною війною, рядом дослідників, зокрема, А. Савчуком, А. Жариковою, О. Радутним, прогнозується подальше зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі. Розширюється коло структур, які намагаються сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі, посилюють державний контроль за національними сегментами мережі Інтернет. При цьому поширюється інструментарій, що передбачає накопичення великих масивів інформації щодо поведінки людини, соціальних груп та використання сучасних досягнень у сфері штучного інтелекту. Посилюється тенденція здійснення розвідувально-підривної діяльності у кіберпросторі шляхом залучення спецслужбами російської федерації, міжнародних хакерських угруповань для реалізації кібервпливу [3, с. 27].

Зростає технічний рівень реалізації кіберзагроз, постійно вдосконалюються та розробляються нові інструменти і механізми кібератак. Посилюється тенденція щодо використання кібератак як інструменту спеціальних інформаційних операцій, маніпулювання суспільною думкою, впливу на виборчі процеси.

Як зазначає експерт А. Жарикова, російська агресія на Україну не обмежилася лише збройними протистояннями. Агресія в кіберпросторі була і раніше, але, починаючи з 2022 року, вона набрала відкритих форм. Разом з тим, перед початком відкритої російської агресії було здійснено низку шпигунських операцій, які мали на меті збір інформації, насамперед, з установ суб'єктів оборонно-безпекового сектору, а також потужних суб'єктів підприємництва. Це надавало можливість владі російської федерації будувати певну стратегію подальших дій, відповідно до відомих планів української сторони. Доречі, найбільшим джерелом хакерських атак протягом 2022-2023 років у світі стає саме російська федерація, яка здійснює більш ніж половину усіх злочинних дій у цій сфері на міжнародному рівні – 58%. За нею КНДР, на яку припадає 23%. Україна займає перше місце серед тих, проти кого вони спрямовані. На Україну припадає 19% усіх світових кібератак. Для контрасту: відсоток кібератак на

Бельгію, Японію та Німеччину не перевищує 3% від загальної світової кількості [4].

Відповідно до звіту Microsoft, росія наростила кіберпотужність за 2022-першу половину 2024 з 21% до 32%. Також було визначено основні галузі, що піддаються атакам. Найбільше зусиль хакерів припадає на сектор держуправління та дипломатії – 48%. До речі, саме на цю сферу зросла увага російських хакерів аж з 3% до 53%. 31% кібератак приймають на себе Збройні Сили та телекомунікаційні системи. З дуже великим відривом в перелік цілей потрапляє освіта – 3% та медіа, охорона здоров'я, ІТ – 1%. Загалом, 2022-2024 роки важко назвати «кіберспокійними» для України. Проте, січень 2022 побив усі рекорди. Лише за один місяць було виявлено та нейтралізовано більше 120 атак, а це лише офіційна статистика. За інформацією СБУ, більшість здійснених кібератак належали до 4 типів: атаки на веб-додатки; шкідливе програмне забезпечення; несанкціоноване з'єднання з командно-контрольними серверами; намагання отримати несанкціонований доступ [4].

Слід, як вбачається, погодитись з поглядами Л. Ю. Веселової та В. В. Зуя, що й досі, не дивлячись на суворі реалії повномасштабної війни, наразі існує проблема недосконалості законодавства у сфері кібербезпеки, застарілість інформаційно-правових норм, недостатній рівень стягнень за інформаційні правопорушення, повільна та несистемна інтеграція положень європейського законодавства в окреслену сферу [5, с. 18; 6, с. 231].

Варто зазначити, що проблематика кібернетичної безпеки та державної політики, спрямованої на її забезпечення, виступає предметом наукових досліджень багатьох вчених, насамперед, фахівців у галузі адміністративного, кримінального права, а також права інтелектуальної власності, зокрема: В. Б. Авер'янова, І. В. Арістової, І. Л. Бачило, І. П. Голосніченка, О. Д. Довганя, Р. О. Додонова, І. М. Дороніна, В. В. Зуй, Л. В. Кузенка, О. Є. Кутафіна, В. Л. Манілова, О. В. Нестеренка, Г. В. Падалка, В. Л. Сидоренко, О. Ю. Синявської, С. Г. Стеценка, С. С. Теленика, М. М. Тищенка, Ю. П. Тихомірова, О. М. Шевчука, В. М. Фурашева, І. О. Харитоненка та інших.

Водночас, аналіз чинного законодавства вказує на те, що існує ряд недоліків щодо регулювання питання кібербезпеки (оборони), які потребують негайного формування пропозицій щодо шляхів вирішення існуючих проблем як з урахуванням потреб забезпечення національної безпеки в умовах повномасштабної війни, так і необхідності європейської інтеграції національного законодавства в цілому. У цьому контексті слушно зазначає С.С. Теленик про те що, держава має виступити ініціатором та гарантом ефективного розвитку і використання інформаційного простору України, особливо в оборонній сфері. Система кібербезпеки повинна бути багаторівневою і надійною, тобто такою, що унеможливить отримання несанкціонованого доступу до відомостей військового характеру, даних, що складають державну таємницю. У зв'язку з цим ряд авторів, зокрема, В. В. Зуй та С. С. Теленик пропонують створити Інформаційний кодекс України, що систематизував би інформаційно-правові норми та, зокрема, більш чітко, детально і змістовно

регулював би питання забезпечення кібербезпеки. Погодимося, що наразі існує проблема недосконалості законодавства у сфері кібербезпеки, застарілість інформаційно-правових норм, недостатній рівень стягнень за інформаційні правопорушення, повільне застосування положень європейського законодавства в даній сфері. Пропонується також формування уніфікованого понятійно-термінологічного апарату у сфері кібербезпеки, а також його узгодження з термінологією чинного українського законодавства та міжнародних актів з питань кібернетичної безпеки [6, с. 233; 7].

Оновлення та розвиток чинного інформаційного законодавства вимагає, на погляд дослідників у сфері кіберзахисту, насамперед, О. М. Суходолі, комплексного підходу, який повинен ґрунтуватись на таких засадах:

- розроблення та впровадження регуляторних механізмів щодо ефективного функціонування нормативного масиву з питань кібербезпеки;
- співпраця з стратегічними союзниками з обміну інформацією, найкращими практиками та ресурсами для забезпечення кібербезпеки;
- розвиток національних засобів захисту інформаційного простору та електронних ресурсів;
- підготовка та реагування на кібератаки, що повинно включати в себе: ідентифікацію, захист, виявлення, реагування та відновлення;
- впровадження загальнодержавної програми забезпечення кіберосвіти та підвищення обізнаності громадян та юридичних осіб з питань кібербезпеки;
- комплексність підходу до кіберзагроз та міжсекторіальне співробітництво;
- постійне оновлення Стратегії забезпечення державної безпеки, Стратегії кібербезпеки та інших галузевих стратегій з метою своєчасного визначення та окреслення механізму реагування на нові виклики у галузі кібернетичної загрози;
- міжгалузевий обмін досвідом та кращими практиками з метою покращення загального рівня кібербезпеки;
- використання спільних ресурсів у процесі міжсекторіального співробітництва (інформаційні бази, технічні засоби та експертні знання);
- забезпечення впровадження комплексних захистів при кібератаках одночасно різних галузей або секторів [8].

Як вже зазначалось концептуально, прогнозування майбутніх загроз в області кібербезпеки є ключовим завданням для забезпечення національної безпеки за цим напрямом. Відповідно, на погляд М. Сироватченко, ключові варто врахувати наступні аспекти:

- активне формування шостого технологічного укладу (біо-, нано-, інфо-, когнотехнологій, їх конвергенцію) та ризики, з якими стикається держава внаслідок упровадження означених новітніх технологій;
- зростання впливу кіберзагроз на функціонування управлінських структур, як національних, так і транснаціональних;
- поділ сфер впливу у кіберпросторі між світовими центрами сили та посилення їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів;

• необхідність створення нового роду військ – кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі супротивника [9].

Певні імперативи застосування законодавства у сфері кібербезпеки та шляхи його розвитку пропонує Стратегія кібербезпеки України. Аналізуючи положення вказаного програмного документу, доцільно акцентувати увагу на таких її аспектах [10; 11]:

- стратегія кібербезпеки визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних; окреслені виклики та загрози повною мірою зберігають свою актуальність і в сучасних умовах правового режиму воєнного стану;

- метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина;

- досягнення мети здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі, - спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки;

- в Україні триває процес становлення системи стратегічних комунікацій. Органами державної влади України здійснено низку організаційних та практичних заходів зі зміцнення власної інституційної спроможності у сфері стратегічних комунікацій, однак не створено дієвого механізму координації і взаємодії між усіма органами державної влади, залученими до здійснення заходів із протидії загрозам в інформаційній сфері. Зазначене послаблює можливості розбудови комплексного стратегічного планування інформаційного потоку, здійснення системної комунікативної діяльності Кабінету Міністрів України, об'єднання всіх ключових суб'єктів у сфері інформаційних відносин, суб'єктів формування і реалізації державної політики щодо ефективного захисту національного інформаційного простору, утвердження позитивного іміджу України, реалізації цілей захисту національної безпеки України в інформаційній сфері [6, с. 234; 10].

Отже, як вбачається, особлива увага забезпечуючи структур повинна приділятись розробкам стратегічних нормативів з питань кібербезпеки, їх регулярному оновленню та контролю виконання відповідного плану заходів

реалізації на основі оцінки ефективності та спроможностей. Для своєчасного поновлення таких нормативів, в Україні необхідно розробити критерії оцінки стану кібербезпеки в державі, особливо в умовах особливих правових режимів, а після проведення відповідного правового аналізу, - визначити ключові напрями формування нової Стратегії кібербезпеки України, що розраховуватиметься на період після 2025 року. Враховуючи міжнародний досвід, включно з фундаментальними рекомендаціями та директивами НАТО та ЄС, основний стратегічний напрям діяльності суб'єктів національної системи кібербезпеки повинен бути спрямований на кіберзахист критичної інформаційної інфраструктури.

Наприкінці варто зазначити, що на даний час Україна перебуває на передовій кібервійни. І хоча ці обставини негативно впливають на наше життя, їх можна використати для тестування нових ідей та технологій у галузі захисту інформації. Досвід, який ми здобуваємо в боротьбі з ворогом, - є безцінним надбанням для розвитку кібернетичної сфери.

Список використаних джерел:

1. Панченко О. Інформаційна складова національної безпеки. *Вісник Національної академії Державної прикордонної служби України*, 2019. Випуск 3. URL: https://www.rdc.org.ua/download/stati/Informational-warehouse.pdf (дата звернення: 02.02.2025).
2. Кириченко Анастасія. Кібербезпека в Україні: шляхи розвитку та можливості. *Укрінформ.* 07 січня 2024. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html (дата звернення: 02.02.2025).
3. Савчук А.В. Кібербезпека в системі національної безпеки України. *Кваліфікаційна (бакалаврська) робота*. 58 с. ДоНУ імені Василя Стуса, Вінниця, 2022. URL: https://jarch.donnu.edu.ua/article/ view/12715/1261883.pdf (lsej.org.ua) (дата звернення: 02.02.2025).
4. Жарикова Анастасія. Кількість кібератак у 2023 році зросла на 16 % – Держспецзв'язку. *Українська правда*. Розділ: Економічна правда. 31 січня 2024. [Інформаційний портал]. URL: https://www.epravda.com.ua/news/2024/01/31/709355 (дата звернення: 02.02.2025).
5. Веселова Л.Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни: *автореф. дис. докт. юр. наук*: 12.00.07; Одеський державний університет внутрішніх справ, 2021. 38 с.
6. Зуй В.В. Актуальні проблеми кібербезпеки в Україні з урахуванням європейської інтеграції. *Південноукраїнський правничий часопис*. Правове забезпечення адміністративної реформи. 4-2022, Ч.1. С. 231-235. URL: http://www.sulj.oduvs.od.ua/archive/2022/4/part_1/35.pdf (дата звернення: 02.02.2025).
7. Теленик С.С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання. *Монографія.* URL: https://jurkniga.ua/contents/derzhavna-sistema-zakhistu-kritichnoi-infrastrukturi-ukraini-kontseptualni-zasadi-administrativno-pravovogo-

regulyuvannya.pdf?srsltid=AfmBOopbP3IBUus1V-aeQGzd7p8muhVRxx5YrBmWgRWWbAIcVnT7JDmq (дата звернення: 02.02.2025).

8. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: *аналітична доповідь* / за ред. О.М. Суходолі. Київ: НІСД, 2020. 28 с.

9. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету «Львівська політехніка»*. Серія: «Юридичні науки». № 1 (41), 2024. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2024/may/34615/sirovatchenko41.pdf (дата звернення: 02.02.2025).

10. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 року №447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 02.02.2025).

11. Проект Стратегії кібербезпеки України (2021 – 2025 роки) «Безпечний кіберпростір – запорука успішного розвитку країни». 27 с. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 02.02.2025).

12. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 року № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016 (дата звернення: 02.02.2025).

13. Ліпкан В.А., Никифорчук Д.Й., Джужа О.М. Боротьба з тероризмом: *навчальний посібник*. К.: Видавничий дім Скіф, 2013. 548 с.

14. Сопілко О.М. Формування підходів до уніфікації понятійно-категоріального апарату інформаційного права. *Часопис Київського університету права*. 2009. № 3. С. 126-132.

15. Біленчук П., Малій М. Космічна й електронна кіберзлочинність: загрози і виклики нового тисячоліття. [Інформаційний портал: LEX: Військовий юрист]. Думка експерта. Опубліковано: 07.10.2019. URL: https://lexinform.com.ua/dumka-eksperta/kosmichna-j-elektronna-kiberzlochynnist-zagrozy-i-vyklyky-novogo-tysyacholittya/ (дата звернення: 02.02.2025).

16. Харитоненко І.О. Правові засади забезпечення кібербезпеки України в умовах цифрового комунікативного середовища. *Часопис Київського університету права*. 2023/2. С. 61-64.