Бриль Дар'я Павлівна,
здобувач ступеня вищої освіти магістра навчально-наукового інституту права та психології 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

ЗАХИСТ КРИТИЧНОЇ ІТ-ІНФРАСТРУКТУРИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

В умовах стрімкої цифровізації суспільства прослідковується певна залежність державних і приватних структур від інформаційно-комунікаційних технологій, внаслідок чого питання захисту критичної ІТ-інфраструктури набуває особливого значення. В узагальненому виді під критичною ІТ-інфраструктурою розуміють сукупність інформаційних систем, ресурсів та сервісів, безперебійне функціонування яких є життєвою необхідністю для забезпечення національної безпеки, економічної стабільності, охорони здоров'я, енергетики, транспорту та інших ключових сфер життєдіяльності держави [3].

Водночас з розвитком цифрового середовища та посиленням глобальної конкуренції держави стикаються з явищем гібридних загроз, що поєднують у собі кібернапади, інформаційно-психологічні операції, економічні диверсії, технічні саботажі та правові маніпуляції. Такі дії мають комплексний характер і спрямовані на підрив стабільності держави, дезорганізацію управління та зниження довіри до суспільних інститутів. У кіберпросторі гібридні загрози проявляються у вигляді масованих атак на державні реєстри, банківську інфраструктуру, системи енергозабезпечення та комунікації [7, с. 3].

Для України дана проблематика є особливо актуальною в умовах воєнного стану та постійного тиску з боку держави-

агресора з використанням гібридних дій, серед яких значну частину становлять кібератаки на органи державної влади, об'єкти енергетики, транспорту та зв'язку.

Одночасно держава здійснює масштабні євроінтеграційні процеси, які передбачають гармонізацію національного законодавства з нормами та стандартами Європейського Союзу у сфері кібербезпеки, зокрема –імплементацію вимог директиви NIS2. Ця директива – новий законодавчий акт Європейського Союзу, спрямований на посилення кібербезпеки шляхом встановлення суворіших вимог до управління ризиками, звітності про інциденти та обов'язкового впровадження заходів безпеки для ширшого кола компаній, що працюють у критичних галузях. Вона замінює попередню директиву NIS 2016 року, розширює сферу її застосування та посилює відповідальність організацій за забезпечення кіберстійкості [1].

Захист критичної ІТ-інфраструктури в Україні ґрунтується на конституційних принципах національної безпеки, верховенства права та захисту інформації. Базовими нормативними актами у цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України», який визначає систему суб'єктів, принципи та механізми забезпечення кіберзахисту [4], та Закон «Про національну безпеку України», що інтегрує питання кіберзагроз у загальну структуру безпеки держави [2]. Важливими стратегічними документами виступають Кіберстратегія України (2021–2025) та Стратегія національної безпеки, що формують політико-правові пріоритети розвитку кіберстійкості [5]. Актуальною залишається потреба у оновленні законодавства відповідно до європейських стандартів NIS2, а також у створенні ефективної системи державного контролю за дотриманням вимог кібербезпеки. Лише чітке нормативне визначення об'єктів критичної ІТ-інфраструктури, підкріплене узгодженими міжвідомчими механізмами, може забезпечити її реальний захист в умовах зростаючих гібридних загроз. Міжнародно-правові документи, зокрема Tallinn Manual та Будапештська конвенція про кіберзлочинність, формують базові підходи до кваліфікації таких дій і визначають механізми співпраці між державами [6].

Проблемним залишається віднесення кібердій до актів агресії або тероризму, адже чинне міжнародне право не має

чітких критеріїв для цього. Водночас дедалі більшого значення набуває явище lawfare – використання правових механізмів як інструменту політичного або воєнного тиску [8].

Таким чином, захист критичної ІТ-інфраструктури в умовах гібридних загроз є стратегічним завданням держави, що поєднує правові, технічні та організаційні заходи. Україна вже створила базові інституційні та нормативні механізми кібербезпеки, однак потребує подальшої гармонізації законодавства з нормами ЄС, запровадження єдиних стандартів кіберзахисту та посилення державно-приватної взаємодії.

Ефективна протидія гібридним загрозам можлива лише за умови міжвідомчої координації, міжнародного партнерства та професійної правової експертизи, спрямованої на забезпечення кіберстійкості держави та суспільства.

Список використаних джерел

1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) : Directive of 14.12.2022.

2. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII : станом на 5 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 08.10.2025).

3. 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 (дата звернення: 11.10.2025).

4. 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 (дата звернення: 10.10.2025).

5. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 12.10.2025).

6. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL:

https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 14.10.2025).

7. Делембовський М., Ткаченко В., Дмитро Д. Захист критичної інфраструктури України від кібератак. *Міжнародний науковий журнал «Грааль науки»*. 2024.

8. Yefimenko I., Sakovskyi A., Bilozorov Ye. Protection of critical infrastructure as a component of Ukraine's national security. *Юридичний часопис НАВС*. Т. 13, № 2, 2023. DOI: 10.56215/naia-chasopis/2.2023.74

Броварник Анна Сергіївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології 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

МІЖНАРОДНИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Щодня в світі, в силу його шаленого темпу розвитку, з'являється багато різних можливостей у кіберпросторі, більшість із яких, відповідно, потребують збору та обробки персональних даних. Варто зауважити, що ні приписи норм законодавства, ні інші важелі суспільного впливу не зможуть забезпечити абсолютну безпеку персональних даних у кіберпросторі, адже витік інформації може статися навіть тоді, коли більшість про це не здогадуєтеся [1, с. 255].

Важливою рисою кіберзлочинності є її глобальний, інтернаціональний характер, що обумовлює низьку ефективність традиційних методів припинення злочинів. Слід зазначити, що для організації ефективної боротьби з кіберзлочинністю держави мають співпрацювати між собою –