

4. Калетнік Г. М. Біопаливо: продовольча, енергетична та екологічна безпека України. Біоенергетика. 2013. № 2. С. 12-14.

5. Україна на шляху до ЄС: реалії та перспективи. Аналітична доповідь. 2022. Український центр економічних та політичних досліджень імені Олександра Розумкова. URL: https://razumkov.org.ua/images/journal/NSD187-188_2022_ukr_full.pdf

DOI <https://doi.org/10.36059/978-966-397-502-3-2>

Лисенко С. Є.,

аспірант кафедри криміналістики та судової медицини

Національної академії внутрішніх справ

м. Київ, Україна

КІБЕРБЕЗПЕКА ПІД ЧАС РОЗСЛІДУВАННЯ НЕЗАКОННОГО ПЕРЕПРАВЛЕННЯ ОСІБ ЧЕРЕЗ ДЕРЖАВНИЙ КОРДОН УКРАЇНИ

У 2017 р. Верховною Радою України прийнято Закон «Про основні засади забезпечення кібербезпеки України», в якому зазначається, що кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1]. Варто відмітити, що частина науковців вважає таке визначення не досить правильним. Так, І. В. Діордіца вказує на те, що помилковість даної конструкції доведена в численних монографіях і дослідженнях, а збереження цієї формули побудови поняття свідчить про небажання авторів нормативно-правових актів дослуховуватись до науковців і їхнє несприйняття обґрунтованих аргументів щодо неправильності і помилковості ототожнення безпеки зі станом захищеності. Науковець переконаний, що кібернетична функція поступово стає однією з основних функцій держави, оскільки кіберпростір є унікальним явищем, яке не має кордоні та об'єднує в собі кібернетичний простір, кібернетичні ресурси, кібернетичну інфраструктуру та кібернетичні технології, а невід'ємним їх складником виступають як кібернетична, так і інформаційна безпека [2, с. 110–111].

Суб'єкти забезпечення кібербезпеки є учасниками не інформаційних, а адміністративних правовідносин, оскільки відносини між

ними будуються на основі влади та підпорядкування, до того ж останні реалізують механізм кіберзахисту шляхом використання примусу, який їм надано чинним законодавством. В. В. Бухарев зауважує, що суб'єктами забезпечення кібербезпеки є державні органи та їхні посадові особи, наділені владними повноваженнями та відповідними обов'язками щодо охорони об'єктів кібербезпеки, котрі знаходяться у законній підпорядкованості між собою [3, с. 88]. У межах своєї компетенції суб'єкти забезпечення кібербезпеки здійснюють: заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; інформаційний обмін щодо реалізованих і потенційних кіберзагроз; розробку і реалізацію запобіжних, організаційних, освітніх та інших заходів у сфері кібербезпеки, кібероборони та кіберзахисту; проведення аудиту інформаційної безпеки у т.ч. на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління; інші заходи із забезпечення розвитку та безпеки кіберпростору [4, с. 120–121].

Зважаючи на те, що до об'єктів кіберзахисту законодавець відносить комунікаційні системи, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади на особливу увагу заслуговують Єдиний реєстр досудових розслідувань та бази даних, що ведуться Державною прикордонною службою України.

Єдиний реєстр досудових розслідувань (далі – ЄРДР) – це електронна інформаційно-комунікаційна система, призначена для збирання, зберігання, захисту, обробки, обліку, пошуку та узагальнення даних, які використовуються для формування звітності, а також надання інформації про відомості, внесені до Реєстру, з дотриманням вимог кримінального процесуального законодавства та законодавства, яким урегульовано питання захисту персональних даних та доступу до інформації з обмеженим доступом. Реєстр утворений та ведеться з метою забезпечення: 1) реєстрації кримінальних правопорушень (проваджень) та осіб, які їх вчинили, обліку прийнятих під час досудового розслідування рішень та результатів судового провадження; 2) оперативного контролю за додержанням законів під час проведення досудового розслідування; 3) формування звітності про стан кримінальної протиправності та результати роботи органів досудового розслідування; 4) аналізу стану та структури кримінальних правопорушень, вчинених у державі; 5) інформаційно-аналітичного забезпечення державних органів, у тому числі правоохоронних та судових відповідно до вимог законодавства [5].

Адміністрація Державної прикордонної служби України є розпорядником системи «Аркан», яка була створена з метою своєчасного,

достовірного та функціонально повного інформаційно-аналітичного забезпечення діяльності суб'єктів системи стосовно здійснення ними заходів із запобігання і недопущення в'їзду в Україну або виїзду з України осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або яких тимчасово обмежено в праві виїзду з України, у тому числі згідно з дорученням правоохоронних органів, розшуку в пунктах пропуску через державний кордон осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, припинення протиправної діяльності фізичних і юридичних осіб, які незаконно переправляють мігрантів в Україну або транзитом переміщують їх через територію України, посилення контролю за додержанням правил в'їзду, виїзду, перебування в Україні іноземців та осіб без громадянства а також виконання інших завдань у правоохоронній сфері згідно із законодавством [6].

Вищевказані системи відповідним чином використовуються під час розслідування незаконного переправлення осіб через державний кордон України, в них накопичується певний обсяг специфічної інформації, а її витік, особливо в теперішніх умовах ведення війни проти Р осії, може призвести до негативних наслідків. У зв'язку з цим, слід використовувати комплекс заходів, що захищатиме ці системи від кібератак і несанкціонованого використання. В цій ситуації орієнтиром повинна бути Постанова Кабінету Міністрів України від 19.06.2019 р. № 518, якою затверджено Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури [7]. Варто виокремити ряд факторів, що, на нашу думку, можуть нести загрозу для інформації у вищезгаданих системах: людський фактор (погано навчені співробітники або такі, що недбало ставляться до роботи з інформацією); фізична небезпека (доступ до інформації повинен бути суворо регламентований та надаватися лише авторизованим особам); внутрішні загрози (стосуються обслуговуючого персоналу); вразливість у програмному забезпеченні (слід проводити роботу щодо вдосконалення програмного забезпечення, його вдосконалення та оновлення); DoS/DDoS-атаки та шкідливе програмне забезпечення (зменшення доступних для атаки зон, використання методів гасіння навантаження на сервер). Саме робота в цих напрямках може забезпечити належний рівень кібербезпеки у роботі як ЄРДР, так і системи «Аркан».

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. (зі змінами). URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення 24.03.2025).
2. Діордіца І. В. Система забезпечення кібербезпеки: сутність та призначення. *Підприємництво, господарство і право*. 2017. № 7. С. 109–116.

3. Бухарев В. В. Адміністративно-правові засади забезпечення кібербезпеки України : дис. ... канд. юрид. наук: 12.00.07. Суми, 2018. 221 с.

4. Тарасюк А. В. Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки ТНУ імені В. І. Вернадського. Серія : Юридичні науки*. 2020. № 2. Т. 31 (70). Ч. 2. С. 119–124.

5. Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення: Наказ Офісу Генерального прокурора від 30.06.2020 р. № 298 (за змінами). URL: <https://zakon.rada.gov.ua/laws/show/v0298905-20#Text> (дата звернення 24.03.2025).

6. Про затвердження Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему, щодо контролю осіб, транспортних засобів та вантажів, які перетинають кордон: Наказ Адміністрації Державної прикордонної служби України, Державної митної служби, Державної податкової адміністрації України, Міністерства внутрішніх справ України, Міністерства закордонних справ України, Міністерства праці та соціальної політики України, Служби безпеки України, Служби зовнішньої розвідки України від 03.04.2008 р. № 284/287/214/150/64/175/266/75. URL: <https://zakon.rada.gov.ua/laws/show/z0396-08#Text> (дата звернення 24.03.2025).

7. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 р. № 518 (зі змінами). URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text> (дата звернення 24.03.2025).

DOI <https://doi.org/10.36059/978-966-397-502-3-3>

Распопов В. Б.,

*кандидат фізико-математичних наук, доцент
Інституту кібернетики імені В. М. Глушкова
Національної академії наук України
м. Київ, Україна*

ДОЛУЧАЙМОСЯ ДО РЕАЛІЗАЦІЇ ПРОЄКТУ «ЦИФРОВІ АВАТАРИ ВИДАТНИХ УКРАЇНЦІВ: В.І. ВЕРНАДСЬКИЙ»

У цифрову епоху штучний інтелект (ШІ) стає цінним інструментом для збереження національної спадщини та розвитку культурних практик в умовах сучасних суспільних викликів. Наприклад,