УДК 343.1
DOI https://doi.org/10.32844/2618-1258.2026.2.24

ВОЛИНЕЦЬ Р.А., ПТАЩЕНКО Д.С.

КВАЛІФІКАЦІЯ ВИКОРИСТАННЯ БОТНЕТ-МЕРЕЖ ДЛЯ АТАК НА ДЕРЖАВНІ ІНФОРМАЦІЙНІ РЕСУРСИ УКРАЇНИ

QUALIFICATION OF THE USE OF BOTNET NETWORKS FOR ATTACKS ON STATE INFORMATION RESOURCES OF UKRAINE

Умови гібридної війни та зростання кількості кібератак на державні інформаційні ресурси України актуалізують необхідність дослідження використання ботнет-мереж як інструменту кіберзлочинності. Масове застосування скомпрометованих пристроїв для несанкціонованого впливу на інформаційні системи держави створює загрозу функціонуванню органів державної влади, державних реєстрів, цифрових сервісів та об'єктів критичної інформаційної інфраструктури. Особливого значення набуває формування єдиного підходу до кримінально-правового аналізу використання ботнет-мереж для атак на державні інформаційні ресурси України. Під час дослідження використано формально-юридичний, системно-структурний, порівняльно-правовий та логіко-семантичний методи. Застосування зазначених методів забезпечило аналіз положень законодавства у сфері кібербезпеки, визначення ознак ботнет-мереж, дослідження змісту поняття державних інформаційних ресурсів та уточнення понятєво-категоріального апарату. Виявлено, що використання ботнет-мереж характеризується розподіленим характером кібератак, прихованим дистанційним керуванням зараженими пристроями та автоматизованим виконанням шкідливих команд. З'ясовано, що основною метою таких атак є порушення конфіденційності, цілісності та доступності державних інформаційних систем. Проаналізовано наукові підходи до визначення державних джерел інформації та запропоновано авторське визначення використання ботнет-мереж для атак на інформаційні ресурси України як умисної протиправної діяльності, спрямованої на несанкціонований вплив на національні комунікаційні системи шляхом використання мережі скомпрометованих пристроїв.

Доведено необхідність удосконалення кримінально-правової кваліфікації використання ботнет-мереж для атак на державні інформаційні ресурси України та нормативного закріплення відповідної дефініції. Реалізація запропонованих підходів сприятиме підвищенню ефективності протидії кіберзлочинності та зміцненню кібербезпеки держави.

Ключові слова: *ботнет-мережі, кіберзлочинність, державні інформаційні ресурси, кібербезпека, кібератаки, несанкціоноване втручання, інформаційна інфраструктура.*

The conditions of hybrid warfare and the growing number of cyberattacks on Ukraine's state information resources necessitate studying the use of botnets as an instrument of cybercrime. The large-scale use of compromised devices for unauthorized interference with state information systems poses a significant threat to the functioning of public

© ВОЛИНЕЦЬ Р.А. – доктор юридичних наук, професор, професор кафедри кримінально-правової політики та кримінального права (Навчально-науковий інститут права Київського національного університету імені Тараса Шевченка) https://orcid.org/0000-0002-8134-8572

© ПТАЩЕНКО Д.С. – кандидат юридичних наук, асистент кафедри кримінально-правової політики та кримінального права (Навчально-науковий інститут права Київського національного університету імені Тараса Шевченка) https://orcid.org/0000-0001-9751-1509

authorities, state registers, digital services, and critical information infrastructure facilities. Particular importance is attached to developing a unified approach to the criminal law assessment of the use of botnets in attacks on Ukraine's state information resources. The study employed formal-legal, system-structural, comparative-legal, and logical-semantic methods. The application of these methods ensured the analysis of cybersecurity legislation, the identification of botnet features, the examination of the concept of state information resources, and the clarification of the conceptual and categorical framework of the research. It was established that botnets are characterized by the distributed nature of cyberattacks, the covert remote control of infected devices, and the automated execution of malicious commands. The study determined that the primary purpose of such attacks is to violate the confidentiality, integrity, and availability of state information systems. Scientific approaches to defining state information resources were analyzed, and the author proposed characterizing the use of botnets to attack Ukraine's state information resources as intentional, unlawful activity aimed at unauthorized interference with state information systems through a network of compromised devices. The necessity of improving the criminal law qualification for the use of botnets in attacks on state information resources of Ukraine and the normative consolidation of the relevant definition have been substantiated. The implementation of the proposed approaches will enhance the effectiveness of combating cybercrime and strengthen the state's cybersecurity.

Key words: *botnet networks, cybercrime, state information resources, cybersecurity, cyberattacks, unauthorized interference, information infrastructure*

Актуальність теми. Умови стрімкої цифровізації державного управління та зростання залежності суспільно важливих процесів від інформаційно-комунікаційних систем зумовлюють суттєве підвищення рівня кіберзагроз, спрямованих на державні інформаційні ресурси України. Особливо небезпечним проявом таких загроз є використання ботнет-мереж як інструменту організації несанкціонованого втручання у роботу інформаційних (автоматизованих) систем, електронних комунікаційних мереж та критичної інформаційної інфраструктури.

Згідно із кримінальним правом зазначені дії підлягають кваліфікації насамперед за статтями 361 та 361-1 Кримінального кодексу України, які визначають відповідальність за несанкціоноване втручання у роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку, зокрема за створення та використання шкідливого програмного забезпечення. Водночас наявна правозастосовна практика не завжди ураховує інфраструктурну природу ботнет-мереж, їхній розподілений характер та здатність до організації масованих координованих атак, що ускладнює правильну кримінально-правову кваліфікацію [11].

Актуальність дослідження зумовлено необхідністю комплексного правового аналізу таких дій, оскільки сучасні підходи до кваліфікації кіберзлочинів не завжди ураховують інфраструктурну природу ботнетів та їхню здатність до одночасного ураження значної кількості цифрових об'єктів. Перспективність дослідження полягає у формуванні точнішого науково-правового інструментарію для протидії складним кіберзагрозам та удосконаленні нормативного регулювання у сфері кібербезпеки [14].

Аналіз сучасних наукових публікацій у сфері кібербезпеки та ботнет-мереж засвідчує зростання уваги до проблем виявлення, класифікації та нейтралізації розподілених інфраструктур кіберзагроз. Дослідники розглядають ботнети як складні динамічні системи, що поєднують автоматизацію, приховане керування та масштабованість атак на інформаційні ресурси.

Зокрема, базові концептуальні підходи до розуміння кібербезпеки та сучасних загроз розробляє О. Летичевський, наголошуючи на комплексному характері кіберзахисту та необхідності поєднання формальних моделей і практичних механізмів протидії атакам [14]. На застосуванні глибокого навчання для прогнозування та виявлення аномалій у кіберінфраструктурі, що є важливим для ідентифікації ботнет-активності, акцентують В. Шульга, І. Іванченко та М. Рижаков [16]. Одночасно використання згорткових нейронних мереж для виявлення DDoS-атак у мережевому трафіку розглядає Є. Майор [15]. А роль штучного інтелекту в інформаційних конфліктах вивчає Ю. Ільченко [13]. Додатково, методи оцінювання захисту корпоративних мереж аналізують А. Ільєнко та В. Ахрамович [12].

Значущими для розв'язання цієї проблематики є закордонні праці. Так, поведінкові характеристики peer-to-peer-ботнетів досліджують А. Г. Г. Кабла із колегами [4], підкреслюючи складність

їхнього виявлення [4]. Відповідно, еволюцію ботнет-загроз в умовах розвитку штучного інтелекту вивчають А. Махбубі зі співавторами [6]. Тоді як підхід до обґрунтованого виявлення IoT-ботнетів пропонують А. А. Корба із колегами [5]. У цьому контексті федеративне навчання для децентралізованого виявлення ботнет-атак вивчають М. А. Госсейн і М. С. Іслам [2]. Ефективність машинного навчання для виявлення IoT-ботнетів демонструють Т. Жукабаєва зі співавторами [10]. Крім того, edge-обчислення для захисту IoT-мереж аналізують Д. Рупанетті та Н. Каабуч [7]. Зокрема, стійкість моделей до adversarial-атак досліджують Р. Юмлембам із колегами [9]. Узагальнюючи, підходи до виявлення IoT-ботнетів пропонують З. Аль-Отман зі співавторами [1]. А механізми виявлення ботнет-активності у реальному часі розробляють Х. Веласко-Мата та колеги [8]. Насамкінець універсальний набір ознак для розпізнавання ботнет-атак пропонують Ф. Гуссейн зі співавторами [3].

Таким чином, аналіз наукових праць демонструє, що сучасні дослідження переважно зосереджено на розвитку інтелектуальних методів виявлення ботнет-мереж, однак залишається нерозв'язаною проблема підвищення універсальності моделей та їхньої стійкості до нових типів кіберзагроз, зокрема атак на державні інформаційні ресурси України.

Об'єктом дослідження є суспільні відносини, що виникають у процесі протидії кіберзлочинності, пов'язаної із використанням ботнет-мереж для атак на державні інформаційні ресурси України.

Мета та завдання дослідження. Метою дослідження є комплексний аналіз правової природи використання ботнет-мереж у кіберзлочинній діяльності та формування науково обґрунтованих підходів до їхньої кваліфікації.

Для досягнення мети дослідження сформульовано такі завдання:

– проаналізувати сутність ботнет-мереж як інструменту кіберзлочинної діяльності та дослідити поняття та структуру державних інформаційних ресурсів;

– характеризувати основні способи використання ботнет-інфраструктур у кібернападах та визначити особливості правової кваліфікації відповідних діянь;

– сформулювати пропозиції щодо удосконалення кримінально-правового регулювання (ст. 361, 361-1 КК України) у частині відповідальності за несанкціоноване втручання у роботу інформаційних систем із використанням ботнет-мереж.

Методи дослідження. У процесі дослідження використано комплекс загальнонаукових та спеціально-правових методів, що забезпечили системний аналіз проблематики використання ботнет-мереж у кіберзлочинній діяльності. Формально-логічний метод застосовано на етапі уточнення базових понять і категорій, зокрема «ботнет-мережа», «кіберзлочин» та «державні інформаційні ресурси», що дало змогу сформувати понятєвий апарат дослідження, тоді як метод аналізу і синтезу – для декомпозиції структури ботнет-інфраструктури та подальшого узагальнення механізмів її функціонування як інструменту розподілених кібератак.

Водночас порівняльно-правовий метод сприяв зіставленню підходів до кримінально-правової кваліфікації несанкціонованого втручання в інформаційні системи в національному законодавстві та окремих закордонних правових моделях, що забезпечило виявлення відмінностей у трактуванні кіберзагроз. Системний метод використано для розгляду ботнет-мереж як елементу ширшої кіберзлочинної інфраструктури у взаємозв'язку із механізмами гарантування інформаційної безпеки держави та функціонуванням критичної інформаційної інфраструктури.

Додатково, формально-юридичний метод уможливив обґрунтування аналізу положень Кримінального кодексу України та спеціального законодавства у сфері кібербезпеки із метою визначення особливостей правової регламентації та кваліфікації діянь, пов'язаних із використанням ботнет-мереж.

Виклад основного матеріалу. Ботнет-мережі є одним із найнебезпечніших засобів здійснення кіберзлочинної діяльності, оскільки забезпечують можливість дистанційного управління великою кількістю скомпрометованих пристроїв для реалізації масштабних атак на інформаційно-комунікаційні системи. Їхнє функціонування ґрунтується на зараженні комп'ютерів, серверів, мобільних телефонів або елементів IoT-інфраструктури спеціальним шкідливим кодом, який забезпечує зловмисникам прихований контроль над технічними засобами користувачів.

Сутність ботнету полягає в об'єднанні інфікованих пристроїв у єдину структуру, здатну виконувати команди координатора без відома власників обладнання. Передавання сигналів керування може здійснюватися через командно-контрольні центри або децентралізовані peer-to-peer-канали взаємодії [14].

Відповідно, кіберзлочинні діяння із залученням ботнет-інфраструктур у правовому вимірі характеризуються сукупністю ознак несанкціонованого доступу та втручання у роботу інформаційних систем, що реалізується шляхом прихованого впливу на програмно-апаратні комплекси без згоди власника чи адміністратора. У цьому контексті значущим є поєднання технічного складника, пов'язаного із функціонуванням скомпрометованих пристроїв, та юридичного компонента, вираженого у свідомому порушенні визначеного режиму експлуатації, правил доступу й стабільності інформаційного середовища [16]. Додатково така діяльність набуває ознак багатоетапного процесу, у межах якого первинне інфікування пристроїв поєднується із подальшим дистанційним керуванням і реалізацією шкідливих команд.

Характерною ознакою ботнет-інфраструктур є розподілений принцип роботи, який дає змогу одночасно використовувати значну кількість пошкоджених вузлів для впливу на визначений об'єкт. Це зумовлює суттєві труднощі для виявлення джерела загрози та ускладнює локалізацію шкідливої активності. Використання великої кількості технічних засобів забезпечує можливість проведення DDoS-атак, незаконного збирання даних, поширення шкідливого програмного забезпечення, реалізації фішингових кампаній і втручання у функціонування державних цифрових сервісів [15].

Ще однією важливою рисою сучасних ботнетів є здатність до адаптації в умовах зміни механізмів кіберзахисту. Використання шифрування, динамічної зміни мережевої поведінки та автоматизованого розподілу команд сприяє мінімізації ризику виявлення. Додаткову небезпеку становить інтеграція технологій машинного навчання та штучного інтелекту, через які оптимізується координація дій пошкоджених пристроїв і здійснюється аналіз уразливостей інформаційних систем.

Саме активна цифровізація публічного управління та розширення використання електронних інформаційних систем сприяють поширенню ботнет-мереж як елементу організованої кіберзлочинної інфраструктури, здатної забезпечувати тривале приховане втручання у функціонування інформаційних систем. Значна частина таких мереж формується за модульним принципом, що забезпечує оперативну зміну механізмів зараження пристроїв, оновлення шкідливих компонентів та адаптацію алгоритмів керування до трансформацій інформаційного середовища. Водночас використання динамічних доменних систем, зашифрованих каналів передавання даних та автоматизованого переміщення командно-контрольних серверів суттєво ускладнює процедури технічного блокування ботнет-інфраструктур.

Крім того, небезпечним є використання ботнетів у поєднанні із технологіями соціальної інженерії. Поширення шкідливого програмного забезпечення може здійснюватися через електронні повідомлення, фальшиві вебресурси, пошкоджені програмні файли або підроблені повідомлення від державних установ. Відповідно, отримання первинного доступу до пристроїв користувачів дає змогу кіберзлочинцям формувати масштабні мережі заражених вузлів, які надалі використовуються для атак на державні цифрові сервіси, системи електронного документообігу та інформаційні комплекси органів влади. Така діяльність створює додаткові ризики компрометації службової інформації та порушення стабільності функціонування державної цифрової інфраструктури.

Особливо критичні наслідки має застосування ботнетів щодо державних інформаційних ресурсів України. Такі дії можуть спричиняти блокування електронних платформ органів влади, порушення доступу до баз даних, дестабілізацію функціонування цифрової інфраструктури, зміну або втрату інформації та створення загроз національній безпеці. Тож, активне упровадження електронного урядування та цифровізація публічного сектору суттєво підвищують рівень уразливості державних систем перед подібними кіберзагрозами [13].

Водночас державні інформаційні ресурси охоплюють упорядковані масиви відомостей, цифрові реєстри, електронні документи, аналітичні платформи та програмно-апаратні комплекси, що використовуються для забезпечення діяльності органів публічної влади. Їхнє функціонування пов'язане із реалізацією управлінських рішень, наданням адміністративних послуг, веденням державного обліку та підтримкою взаємодії між різними інституціями [12]. Значну частину таких ресурсів інтегровано у єдине цифрове середовище, у межах якого здійснюється обмін службовими даними, оброблення запитів і забезпечення електронної комунікації між державою та громадянами (табл. 1).

Наведена структура державних інформаційних ресурсів засвідчує їхній багаторівневий характер та критичне значення для забезпечення безперервності публічного управління, функціонування цифрових сервісів і підтримки національної безпеки. Уразливість таких

Таблиця 1

Структура державних інформаційних ресурсів України та приклади їхнього функціонування

Складник державних інформаційних ресурсів	Характеристика	Приклади
Автоматизовані системи документообігу	Забезпечують електронний обіг службових документів, контроль виконання управлінських рішень, координацію внутрішньої діяльності органів влади та збереження цифрових архівів	Системи електронного документообігу Кабінету Міністрів України, електронний документообіг органів місцевого самоврядування
Електронні бази персональних даних	Містять структуровані відомості про фізичних і юридичних осіб, використовуються для державного обліку, надання адміністративних послуг та ідентифікації громадян	Єдиний державний демографічний реєстр, Державний реєстр актів цивільного стану громадян
Урядові вебпортали та цифрові сервіси	Призначені для забезпечення електронної взаємодії населення із державними установами, подання заяв, отримання довідок і доступу до публічної інформації	Портал «Дія», офіційні вебсайти центральних органів виконавчої влади
Телекомунікаційні вузли та мережеві комплекси	Використовуються для передавання інформації між державними установами, підтримки цифрового зв'язку та функціонування захищених каналів комунікації	Урядова мережа спеціального зв'язку, державні серверні комунікаційні системи
Центри зберігання та оброблення інформації	Забезпечують накопичення, резервування, оброблення та захист великих обсягів даних, необхідних для стабільної роботи державних електронних ресурсів	Датацентри державних органів, хмарні платформи зберігання службової інформації
Інформаційні комплекси сектору безпеки й оборони	Використовуються для координації діяльності правоохоронних органів, оборонного сектору та спеціальних служб у сфері національної безпеки	Інформаційні системи Збройних сил України, аналітичні комплекси Служби безпеки України
Об'єкти критичної цифрової інфраструктури	Забезпечують функціонування стратегічно важливих сфер держави, порушення роботи яких може спричинити масштабні негативні наслідки	Інформаційні системи енергетичного сектору, банківські платіжні мережі, державні транспортні цифрові комплекси

Джерела: систематизовано автором.

компонентів до зовнішнього кібернетичного впливу створює підвищені ризики для стабільності державних інституцій, особливо за умов активного використання організованими групами шкідливого програмного забезпечення та мереж заражених пристроїв. З огляду на це проблема застосування ботнет-мереж набуває не лише технічного, а й кримінально-правового значення, оскільки подібні дії спрямовуються на порушення функціонування інформаційної інфраструктури, блокування доступу до електронних ресурсів та завдання шкоди державним цифровим системам.

Оскільки функціонування державних інформаційних ресурсів забезпечує реалізацію значної кількості управлінських, фінансових, безпекових та соціальних процесів, пов'язаних із діяльністю органів державної влади, то порушення стабільності роботи цифрових систем може

спричиняти затримки у наданні адміністративних послуг, блокування доступу до державних реєстрів, дестабілізацію електронної взаємодії між органами влади та створення ризиків втрати критично важливої інформації. Суттєві ризики зумовлюють кібератаки на інформаційні комплекси сектору безпеки й оборони, телекомунікаційні вузли та державні системи електронної ідентифікації громадян.

Додаткову загрозу становить висока інтегрованість державних цифрових платформ, у межах якої ураження одного елемента інформаційної інфраструктури може впливати на функціонування суміжних систем. Зокрема, використання ботнет-мереж для реалізації комплексних кібератак створює ризик одночасного блокування декількох державних сервісів, перевантаження центрів оброблення даних та порушення електронної комунікації між державними установами. За таких умов забезпечення кіберстійкості державних інформаційних ресурсів набуває стратегічного значення для підтримки безперервності функціонування публічного управління та захисту національних інтересів України.

У правовому аспекті використання ботнет-структур поєднує декілька форм протиправної діяльності: незаконне втручання у роботу інформаційних систем, створення та поширення шкідливого програмного забезпечення, порушення функціонування електронно-комунікаційних мереж та несанкціоноване отримання інформації. Транснаціональний характер таких дій, складність виявлення організаторів і використання анонімізованих каналів зв'язку істотно ускладнюють процес юридичної кваліфікації та механізми притягнення винних осіб до відповідальності.

Таке несанкціоноване втручання у функціонування інформаційних систем, електронних комунікаційних мереж та інформаційно-комунікаційної інфраструктури є однією з найнебезпечніших форм кіберзлочинної діяльності, що безпосередньо пов'язана із застосуванням ботнет-мереж. Кримінально-правова відповідальність за такі дії передбачена ст. 361 Кримінального кодексу України (КК України), яка охоплює незаконний вплив на процеси оброблення інформації, блокування доступу до ресурсів, спотворення даних або порушення визначеного порядку маршрутизації [11]. А використання заражених пристроїв для масового надсилання запитів, перевантаження серверів чи координації DDoS-атак створює загрозу стабільності функціонування державних цифрових платформ та критичної інфраструктури.

Важливим інструментом у протидії ботнет-загрозам є ст. 361-1 КК України, яка визначає відповідальність за створення, поширення, використання або збут шкідливих програмних чи технічних засобів. Саме через спеціалізоване програмне забезпечення здійснюється зараження пристроїв, приховане отримання контролю над ними та подальше дистанційне керування. Функціонування ботнету передбачає координацію великої кількості пошкоджених вузлів, здатних виконувати команди організатора без відома власників обладнання, що значно підвищує масштабність і небезпечність кібернападів.

Проте складність кримінально-правової кваліфікації зазначених діянь обумовлено транскордонним характером кіберзлочинності, використанням анонімних каналів зв'язку, VPN-технологій, проксі-серверів та розподілених цифрових платформ. Суб'єктність характеризується прямим умислом, оскільки втручання у роботу інформаційної інфраструктури здійснюється цілеспрямовано для блокування державних сервісів, незаконного отримання доступу до даних або дестабілізації діяльності органів влади. Використання ботнет-мереж як інструменту кібератак демонструє високий рівень організованості протиправної діяльності та потребує удосконалення механізмів кримінально-правового реагування у сфері кібербезпеки [4].

Відповідно, окремого значення набуває проблема окреслення меж кримінальної відповідальності учасників ботнет-інфраструктур. Організація та функціонування подібних мереж передбачає розподіл ролей між особами, які здійснюють розроблення шкідливого програмного забезпечення, адміністрування командно-контрольних серверів, поширення заражених файлів та безпосередню координацію кібератак. Наявність декількох рівнів взаємодії між учасниками ускладнює визначення ступеня участі кожного суб'єкта у вчиненні кримінального правопорушення та потребує комплексного оцінювання їхнього функціонального внеску у реалізацію кіберзлочинної діяльності.

Одночасно проблематика правозастосування пов'язана із використанням орендованих ботнет-мереж у межах моделі «botnet-as-a-service», відповідно до якої доступ до зараженої інфраструктури надається третім особам за винагороду. Подібні механізми сприяють поширенню кіберзлочинної діяльності серед широкого кола користувачів, які не мають спеціальних технічних навичок, проте отримують можливість організовувати DDoS-атаки, здійснювати

несанкціоноване втручання у функціонування інформаційних систем або поширювати шкідливе програмне забезпечення. Ці схеми потребують удосконалення підходів до кваліфікації співучасті у кіберзлочинах та адаптації кримінального законодавства до нових форм функціонування цифрової злочинності.

Такі сформовані ботнет-інфраструктури використовуються для реалізації широкого спектра кібернападів, спрямованих на порушення стабільного функціонування інформаційних систем, отримання несанкціонованого доступу до даних та дестабілізацію роботи державних електронних ресурсів. Найпоширенішими способами їхнього застосування є організація DDoS-атак, масове розповсюдження шкідливого програмного забезпечення, перехоплення конфіденційної інформації та використання заражених пристроїв для прихованого доступу до інформаційної інфраструктури держави.

Правова кваліфікація таких діянь потребує визначення форми несанкціонованого втручання, способу використання шкідливих технічних засобів та характеру суспільно небезпечних наслідків. Залежно від конкретних обставин застосовуються положення ст. 361 та 361-1 КК України [11] та суміжні склади кримінальних правопорушень у сфері незаконного збирання інформації або порушення роботи електронних комунікаційних мереж. Складність цієї кваліфікації обумовлена прихованим характером кібердіяльності, використанням розподілених мереж заражених пристроїв та транснаціональним розміщенням елементів кіберінфраструктури, що ускладнює виявлення суб'єкта злочину та доказування його участі в організації атаки.

Додатково, одним із найпоширеніших проявів використання ботнет-мереж є DDoS-атаки на державні вебпортали та електронні сервіси шляхом одночасного генерування значних обсягів запитів, що призводить до перевантаження серверних ресурсів і тимчасового обмеження доступу користувачів до державних цифрових послуг [8]. Подібні діяння становлять підвищену суспільну небезпеку для систем електронного урядування, фінансової та енергетичної інфраструктури, оскільки можуть спричиняти порушення управлінських процесів і значні економічні втрати.

Ще одним способом сформувати загрози є поширення шкідливого програмного забезпечення через фішингові повідомлення або експлуатацію вразливостей мережевого обладнання, що забезпечує несанкціонований доступ до інформаційних систем та подальше використання заражених вузлів для нових атак [2]. За таких умов ботнет-мережі можуть застосовуватися для викрадення облікових даних, проникнення у внутрішні державні мережі або розгортання програм-вимагачів, які блокують доступ до інформаційних ресурсів.

Відповідно до цих ризиків практика протидії кіберзлочинності засвідчує, що ботнет-інфраструктури використовуються одночасно для координації комплексних атак на об'єкти критичної інформаційної інфраструктури, поєднуючи перевантаження систем, приховування джерела втручання та маскування наслідків протиправної діяльності. Це ускладнює розслідування кримінальних правопорушень, оскільки окремі елементи кіберінфраструктури можуть бути розміщені у різних юрисдикціях, а керування здійснюється дистанційно через розподілені канали зв'язку [10]. Відтак ефективне кримінально-правове оцінювання таких діянь потребує комплексного врахування способу вчинення, ролі учасників та наслідків для інформаційної безпеки держави.

Таким чином, удосконалення нормативного забезпечення у сфері протидії ботнет-інфраструктурам потребує насамперед чіткого визначення базових понять у законодавстві. Запропоновано закріплення визначення терміна «ботнет-мережа» як розподіленої системи скомпрометованих пристроїв із прихованим дистанційним керуванням, що використовується для реалізації кіберзагроз. Така нормативна конкретизація усуне неоднозначність під час правозастосування та забезпечить уніфіковані критерії кваліфікації протиправних дій у сфері інформаційної безпеки.

Подальші зміни мають охоплювати посилення кримінально-правової відповідальності за створення, адміністрування й використання подібних мереж, особливо у випадках впливу на державні цифрові системи та критичну інфраструктуру. Передбачення кваліфікаційних ознак, пов'язаних із масштабом ураження, кількістю заражених пристроїв, транснаціональним характером операцій і спрямованістю на порушення стабільності інформаційних ресурсів, дасть змогу точніше відображати ступінь суспільної небезпеки та диференціювати санкції залежно від наслідків.

Додаткового регулювання потребують процесуальні механізми виявлення й фіксації кіберінцидентів. Важливим напрямом є упровадження уніфікованих стандартів цифрової криміналістики, розширення міжнародного обміну технічною інформацією та посилення взаємодії між державними органами й провайдерами електронних комунікацій. Дотримання обов'язкових процедур моніторингу мережевих аномалій сприятиме своєчасному реагуванню на кібератаки та мінімізації їхніх наслідків для державної інформаційної інфраструктури.

Тож, ефективна протидія використанню ботнет-мереж потребує комплексного поєднання правових, організаційних та технічних заходів кіберзахисту. Одним із пріоритетних напрямів є розвиток систем раннього виявлення мережевих аномалій, здатних автоматично фіксувати ознаки масового генерування підозрілих запитів, нехарактерної активності користувачів або спроб несанкціонованого доступу до державних інформаційних ресурсів. Важливе значення має застосування механізмів постійного аудиту інформаційної безпеки та регулярного тестування державних цифрових систем на наявність технічних уразливостей.

Ще одним важливим напрямом залишається підвищення рівня міжнародної співпраці у сфері обміну інформацією про кіберінциденти та координації діяльності щодо ліквідації ботнет-інфраструктур. Саме транснаціональний характер функціонування мереж заражених пристроїв обумовлює необхідність оперативної взаємодії між правоохоронними органами, спеціальними службами, CERT-командами та суб'єктами гарантування кібербезпеки різних держав. Розширення міжнародного співробітництва сприятиме удосконаленню механізмів виявлення організаторів кібератак, блокуванню командно-контрольних центрів і мінімізації загроз для державної інформаційної інфраструктури України.

Висновки. Отримані результати дослідження узгоджуються із науковими працями, у межах яких ботнет-мережі визначаються як складні розподілені кіберінфраструктури, здатні забезпечувати масштабовані та приховані кібератаки на інформаційні системи [6; 10]. На відміну від праць, присвячених переважно технічним аспектам виявлення ботнет-активності [8; 10], роботу зосереджено на проблематиці кримінально-правової кваліфікації використання ботнет-мереж для атак на державні інформаційні ресурси України, що дало змогу розширити наукове розуміння правової природи відповідних кіберзагроз.

Зокрема, підтверджено наукові положення щодо багаторівневого характеру кіберзагроз та складності їхнього виявлення в умовах розподіленої цифрової інфраструктури [7]. Водночас визначено, що використання ботнет-мереж як централізовано керованої системи заражених пристроїв формує підвищений рівень суспільної небезпеки, оскільки забезпечує можливість одночасного впливу на значну кількість державних інформаційних ресурсів, електронних сервісів та об'єктів критичної інформаційної інфраструктури. Так, дослідження сприяло виявленню недостатньої конкретизації ознак використання ботнет-мереж у положеннях ст. 361 та ст. 361-1 КК України, що ускладнює практику кримінально-правової кваліфікації відповідних діянь.

Узагальнення результатів закордонних наукових джерел засвідчило домінування технічного напряму вивчення ботнет-мереж, зокрема розроблення механізмів виявлення, блокування та нейтралізації ботнет-активності [1; 2]. У роботі обґрунтовано необхідність поєднання технічного та кримінально-правового аналізу, оскільки використання ботнет-мереж охоплює не лише технічне втручання у функціонування інформаційних систем, а й ознаки організованої кіберзлочинної діяльності. З'ясовано, що застосування ботнет-інфраструктур супроводжується використанням шкідливого програмного забезпечення, несанкціонованим втручанням у роботу інформаційних систем та порушенням функціонування державних цифрових ресурсів, що потребує комплексного правового аналізу способу вчинення кримінального правопорушення, характеру наслідків і ролі учасників кіберзлочинної діяльності.

Результати дослідження підтвердили, що застосування ботнет-мереж у кібератаках на державні інформаційні ресурси доцільно розглядати як форму організованої кіберзлочинної діяльності, яка охоплює ознаки кримінальних правопорушень, передбачених ст. 361 та ст. 361-1 КК України. Підтверджено, що складність кваліфікації відповідних діянь обумовлено розподіленим характером ботнет-інфраструктури, транснаціональним розміщенням її елементів, використанням анонімізованих каналів зв'язку та багаторівневою структурою взаємодії учасників кібероперацій.

Практичне значення дослідження полягає у можливості використання сформульованих положень у діяльності органів досудового розслідування, судових органів та суб'єктів гарантування кібербезпеки під час кваліфікації кримінальних правопорушень, пов'язаних із використанням ботнет-мереж. Запропоновані підходи можуть бути використані для удосконалення правозастосовної практики, уточнення критеріїв розмежування суміжних складів кримінальних правопорушень у сфері кібербезпеки та підготовки змін до кримінального законодавства України.

У результаті проведеного дослідження виявлено, що ботнет-мережі становлять один із найнебезпечніших інструментів сучасної кіберзлочинності, використання якого створює загрозу

стабільності функціонування державних інформаційних ресурсів та критичної цифрової інфраструктури України. Визначено основні ознаки ботнет-інфраструктур, зокрема розподілений характер функціонування, дистанційне приховане керування зараженими пристроями, автоматизоване виконання шкідливих команд та здатність до масштабування кібератак. Доведено, що використання ботнет-мереж для атак на державні інформаційні ресурси охоплює ознаки несанкціонованого втручання у роботу інформаційних систем та використання шкідливих програмних засобів, що обумовлює необхідність комплексної кримінально-правової кваліфікації відповідних діянь.

Обґрунтовано доцільність нормативного закріплення дефініції використання ботнет-мереж для атак на державні інформаційні ресурси України та вдосконалення кримінально-правових механізмів протидії відповідним формам кіберзлочинної діяльності. Перспективи подальших досліджень пов'язані з аналізом міжнародного досвіду протидії ботнет-інфраструктурам, розробленням уніфікованих механізмів кваліфікації розподілених кібератак та удосконаленням міжнародної взаємодії у сфері боротьби із транскордонною кіберзлочинністю.

Список використаних джерел:

1. Al-Othman, Z., Alkasassbeh, M., & AL-Haj Baddar, S. (2020). A state-of-the-art review on IoT botnet attack detection. *arXiv preprint*, arXiv:2010.13852. https://doi.org/10.48550/arXiv.2010.13852

2. Hossain, M. A., & Islam, M. S. (2025). Towards decentralized cybersecurity: a novel privacy-preserving federated learning approach for botnet attack detection. *Blockchain: Research and Applications*, 100355. https://doi.org/10.1016/j.bcra.2025.100355

3. Hussain, F., Abbas, S. G., Fayyaz, U. U., Shah, G. A., Toqeer, A., & Ali, A. (2020). Towards a universal features set for IoT botnet attacks detection. *arXiv preprint*, arXiv:2012.00463. https://doi.org/10.48550/arXiv.2012.00463

4. Kabla, A. H. H., Thamrin, A. H., Anbar, M., Manickam, S., & Karuppayah, S. (2024). Peer-to-peer botnets: exploring behavioural characteristics and machine/deep learning-based detection. *EURASIP Journal on Information Security*, *2024,* 20. https://doi.org/10.1186/s13635-024-00169-0

5. Korba, A. A., Diaf, A., Bouchiha, M. A., & Ghamri-Doudane, Y. (2025). Mitigating IoT botnet attacks: An early-stage explainable network-based anomaly detection approach. *Computer Communications*, *241*, 108270. https://doi.org/10.1016/j.comcom.2025.108270

6. Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Camtepe, S., Ansari, K., & Barry, B. (2025). The evolving threat landscape of botnets: Comprehensive analysis of detection techniques in the age of artificial intelligence. *Internet of Things*, *33*, 101728. https://doi.org/10.1016/j.iot.2025.101728

7. Rupanetti, D., & Kaabouch, N. (2025). Leveraging machine learning for botnet attack detection in edge-computing assisted IoT networks. *arXiv preprint,* arXiv:2508.01542. https://doi.org/10.48550/arXiv.2508.01542

8. Velasco-Mata, J., González-Castro, V., Fidalgo, E., & Alegre, E. (2023). Real-time botnet detection on large network bandwidths using machine learning. *Scientific Reports*,*13,* 4282. https://doi.org/10.1038/s41598-023-31260-0

9. Yumlembam, R., Issac, B., Jacob, S. M., & Yang, L. (2024). Comprehensive botnet detection by mitigating adversarial attacks, navigating the subtleties of perturbation distances and fortifying predictions with conformal layers. *arXiv preprint,* arXiv:2409.00667. https://doi.org/10.48550/arXiv.2409.00667

10. Zhukabayeva, T., Zholshiyeva, L., Ven-Tsen, K., Adamova, A., Mardenov, Y., & Karabayev, N. (2024). Enhancing IoT security: effective botnet attack detection through machine learning. *Procedia Computer Science*, *241,* 421–426. https://doi.org/10.1016/j.procs.2024.08.058

11. Кримінальний кодекс України від 05.04.2001 № 2341-III. https://zakon.rada.gov.ua/laws/show/2341-14#Text

12. Ільєнко А., Ахрамович В. Метод розрахунку захисту корпоративної мережі в умовах невизначеності. *Кібербезпека: освіта, наука, техніка, 2025.* № 1(29). С. 480–492. https://doi.org/10.28925/2663-4023.2025.29.894

13. Ільченко Ю. О. Застосування технологій штучного інтелекту в інформаційній війні рф проти України. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2025. № 3(91). С. 87–93. https://doi.org/10.24144/2307-3322.2025.91.3.13

14. Летичевський О. О. Сучасні наукові проблеми кібербезпеки. *Вісник Національної академії наук України*. 2023. № 2. С. 12–20. https://doi.org/10.15407/visn2023.02.012

15. Майор Є. Виявлення шкідливих пакетів та DDoS-атак у мережевому трафіку за допомогою глибоких згорткових нейронних мереж. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2024. № 1. С. 303–311. https://doi.org/10.31891/2219-9365-2024-77-41

16. Шульга В., Іванченко І., Рижаков М. Узагальнена модель інтелектуальної системи прогнозування та виявлення аномалій у кіберінфраструктурі на основі глибокого навчання. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2025. № 3. С. 217–225. https://doi.org/10.31891/2219-9365-2025-83-28

Дата першого надходження статті до видання: 06.02.2026
Дата прийняття статті до друку після рецензування: 05.03.2026
Дата публікації (оприлюднення) статті: 20.03.2026