Кримінальне право та кримінологія; кримінально-виконавче право

УДК 343.9

Оболенцев Валерій Федорович

кандидат юридичних наук, доцент,

доцент кафедри кримінально-правової політики

Національний юридичний університет імені Ярослава Мудрого

Obolentsev Valeriy

PhD, Associate Professor,

Associate Professor Department of criminal and legal policy

Yaroslav Mudryi National Law University

ORCID: 0000-0001-8360-8959

ФОРМАЛІЗАЦІЯ ПРОБЛЕМИ ЗЛОЧИННОСТІ НА ЗАСАДАХ МЕТОДИКИ СИСТЕМНОГО АНАЛІЗУ. ЧАСТИНА 2: КІБЕРЗЛОЧИННІСТЬ

FORMALIZATION OF THE CRIME PROBLEM ON THE BASIS OF THE METHODOLOGY OF SYSTEMS ANALYSIS. PART 2: CYBERCRIME

Анотація. *Вступ. На цей час проблема кіберзлочинності сягнула планетарних масштабів. В Україні ж кіберзлочини стали складовою частиною агресії з боку рф. Їх мета співпадає із загальною метою країни агресорки – знищення української державності. Основною мішенню атак є цивільна інфраструктура, енергетичний сектор, медіа та структурні елементи телекомунікації. Тактичні ж пріоритети обираються відповідно до запитів військових.*

Тож кіберзлочинність є актуальною проблемою українського суспільства, а наукове обґрунтування запобіжних заходів щодо злочинів у

сфері інформаційних технологій залишається нагальним завданням вітчизняних науковців.

Мета. Метою статті визначено формалізацію на засадах системотехніки тих проблем, які обумовлює кіберзлочиність у системі держави України.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правові акти щодо визначення кіберзлочинів та заходів їх запобігання; 2) наукові публікації вітчизняних та зарубіжних авторів, що здійснюють свої дослідження щодо кіберзлочинності та заходів її запобігання.

В процесі дослідження використано наукові методи: теоретичного узагальнення – для характеристики напрацювань науковців щодо проблематики кіберзлочинів; аналізу документів – щодо дослідження нормативних першоджерел; системного аналізу – для формалізації проблеми кіберзлочинності у системі держави України; логічного синтезу – для формулювання висновків.

Результати. У науковій статті формалізовано кіберзлочинність як проблему системи держави України. Окреслено три варіанти її прояву: проблеми недосягнення мети у зв'язку з внутрішнім станом системи (зокрема – з причини невідповідності функцій, параметрів системи призначенню або меті системи); проблеми недосягнення мети у зв'язку з внутрішнім станом системи (зокрема – з причини невідповідності меті системи її структури і процесів взаємодії окремих частин); проблеми недосягнення мети, обумовлені відхиленнями у взаємодії системи з середовищем (шкідливий вплив зовнішнього середовища на систему або неналежний вплив системи на її зовнішнє середовище).

Окреслено детермінацію проблем, що існують у системі держави України у зв'язку з кіберзлочинністю.

Перспективи. Формалізація проблеми кіберзлочинності відносно системи держави України орієнтує заходи запобіжної діяльності. У подальших наукових дослідженнях пропонується зосередити увагу на заходах запобігання що мають враховувати фактори детермінації досліджуваного явища-проблеми.

Ключові слова: *кіберзлочинність, кіберзлочини, запобігання кіберзлочинності, система держави, система злочинності, системний аналіз.*

Summary. *Introduction. At this time, the problem of cybercrime has reached planetary proportions. In Ukraine, cybercrime has become an integral part of aggression by the Russian Federation. Their goal coincides with the general goal of the aggressor country - the destruction of Ukrainian statehood.*

The main targets of attacks are civilian infrastructure, the energy sector, media, and telecommunications infrastructure. Tactical priorities are chosen according to military requirements.

Therefore, cybercrime is a pressing problem of Ukrainian society, and the scientific substantiation of preventive measures against crimes in the field of information technology remains an urgent task for domestic scientists.

Purpose. The purpose of the article is to formalize, on the basis of systems engineering, the problems caused by cybercrime in the system of the state of Ukraine.

Materials and methods. The research materials are: 1) regulatory and legal acts on the definition of cybercrimes and measures to prevent them; 2) scientific publications of domestic and foreign authors conducting their research on cybercrimes and measures to prevent them.

In the process of conducting the research, scientific methods were used: theoretical generalization - to characterize the work of scientists on the issues of

cybercrime; document analysis - to study regulatory primary sources; system analysis - to formalize the problem of cybercrime in the system of the state of Ukraine; logical synthesis - to formulate conclusions.

Results. The scientific article formalizes cybercrime as a problem of the system of the state of Ukraine. Three variants of its manifestation are outlined: the problem of failure to achieve the goal due to the internal state of the system (in particular, due to the inconsistency of the functions, parameters of the system with the purpose or purpose of the system); the problem of failure to achieve the goal due to the internal state of the system (in particular, due to the inconsistency of the system's structure and processes of interaction of individual parts with the goal); problems of failure to achieve the goal due to deviations in the interaction of the system with the environment (harmful impact of the external environment on the system or improper impact of the system on its external environment).

The determination of the problems that exist in the system of the state of Ukraine in connection with cybercrime is outlined.

Discussion. Formalization of the problem of cybercrime in relation to the system of the state of Ukraine orients preventive measures. In further scientific research, it is proposed to focus on preventive measures that should take into account the factors determining the phenomenon-problem under study.

Key words: *cybercrime, cybercrimes, cybercrime prevention, state system, crime system, systems analysis.*

Постановка проблеми. Ще у 2001 р. Рада Європи своїм рішенням [6] визначила, що небезпека кіберзлочинів визначається їх спрямованістю проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, прав та свобод громадян з ними пов'язаних. Відтоді рівень кіберзлочинності у Світі значно збільшився у зв'язку з

поширенням цифрових технологій. І станом на цей час ця проблема сягнула планетарних масштабів [1].

В Україні ж кіберзлочини стали складовою частиною агресії з боку рф [18]. Їх мета співпадає із загальною метою країни агресорки – знищення української державності. Основною мішенню атак є цивільна інфраструктура, енергетичний сектор, медіа та структурні елементи телекомунікації. Тактичні ж пріоритети обираються відповідно до запитів військових. Базовим методом російських кібератак залишається таргетований фішинг [2].

Тож кіберзлочинність є актуальною проблемою українського суспільства, а наукове обґрунтування запобіжних заходів щодо злочинів у сфері інформаційних технологій залишається нагальним завданням українських науковців.

Аналіз останніх досліджень і публікацій. Вітчизняні фахівці вже мають суттєві напрацювання щодо протидії кіберзлочинам. Досліджується, зокрема, проблема адаптації заходів кримінально-правової протидії кіберзлочинам (Красько М.І та Цевух А.І.) [7], використання передових технологій у розслідуванні кіберзлочинів (Дунаєва Т. Є.) [5]. Особливу увагу науковці приділяють запобіганню кіберзлочинів в умовах воєнного стану в Україні (Бодунова О. М.) [3].

Узагальнюючи наведені та інші роботи фахівців щодо заходів запобігання кібезлочинів можемо стверджувати, що вони ґрунтуються на загальновизнаній вітчизняній концепції протидії злочинності [4]. Втім, перспективним напрямком окресленої проблематики нам вбачаються наукові пошуки з використанням методики системного аналізу. Підставою для такого твердження є напрацювання профільних науковців [8], власний

досвід системного аналізу злочинності, її детермінації та антикриміногенних заходів [12; 13; 14; 15; 16].

Мета статті. З урахуванням наведеного метою статті визначено формалізацію (на засадах системотехніки) проблеми кіберзлочиності у системі держави України.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правові акти щодо визначення кіберзлочинів та заходів їх запобігання; 2) наукові публікації вітчизняних та зарубіжних авторів, що здійснюють свої дослідження щодо кіберзлочинності та заходів їх запобігання.

В процесі дослідження було використано наукові методи: теоретичного узагальнення – для характеристики напрацювань науковців щодо проблематики кіберзлочинів; аналізу документів – щодо дослідження нормативних першоджерел; системного аналізу – для формалізації проблеми кіберзлочинності у системі держави України; логічного синтезу – для формулювання висновків.

Виклад основного матеріалу. У теорії системотехніки проблема визначається як різниця між потрібним (очікуваним, бажаним, запланованим) та фактичним станом системи (результатами її функціонування) [8, с. 208-209].

Належне функціонування системи передбачає своєчасне досягнення мети системи – у визначені терміни та з раціональними витратами. Недосягнення ж мети з цими параметрами являє собою проблеми у трьох варіантах:

1) проблеми недосягнення мети у зв'язку з внутрішнім станом системи (зокрема – з причини невідповідності функцій, параметрів системи призначенню системи або її меті);

2) проблеми недосягнення мети у зв'язку з внутрішнім станом системи (зокрема – з причини невідповідності меті системи структури і процесів взаємодії окремих частин);

3) проблеми недосягнення мети, обумовлені відхиленнями у взаємодії системи з середовищем (шкідливий вплив зовнішнього середовища на систему або неналежний вплив системи на її зовнішнє середовище) [8, с. 209; 21, с. 139-140].

Згідно вказаного обґрунтування проблемності кіберзлочинності в Україні вбачаємо за доцільне здійснювати відносно системи нашої держави (було розкрито нами раніше [13]), у трьох змістовних форматах.

1. Перший формат проблеми кіберзлочинності у системі держави України - проблеми у внутрішньому стані цієї системи. Тут йдеться про невідповідність функцій призначенню системи. Функція відповідно до теорії системотехніки розуміється як зовнішній прояв властивостей об'єкта в існуючий системі відносин, здатність до дії, роль, вплив, задоволення потреб, обов'язки [9, с. 28]. Тож системною функцією держави Україна є діяльність з утвердження і забезпечення прав і свобод людини, що відповідно до ст. 3 Конституції України є головним *обов'язком* держави. Утвердження прав і свобод можна розуміти як їх формальну інституалізацію у нормативних актах. Забезпечення прав і свобод вбачається як діяльність з їх підтримки за допомогою матеріальних, енергетичних та інформаційних ресурсів.

Функції держави з утвердження й забезпечення прав і свобод реалізуються у процесі діяльності державних органів відповідно до їх відомчої компетенції. Зокрема, політична функція – це забезпечення функціонування демократичних політичних інститутів, економічна функція – забезпечення механізмів ринкової економіки, соціальна функція –

соціальний захист населення, функція охорони правопорядку – забезпечення виконання нормативних приписів учасниками суспільних відносин через заходи превенції правопорушень і т.ін.

Призначенням у теорії системотехніки стверджується декларована здатність системи виконувати функції, що забезпечують досягнення мети [9, с. 27]. Тож призначенням системи держави Україна є гарантування прав і свобод людини - зміст державної діяльності відповідно до ст. 3 Конституції України. Йдеться про створення умов для їх безперешкодної реалізації та відновлення у випадках порушень.

Кіберзлочинність як проблему невідповідності функцій системи держави Україна її призначенню можна пояснити у такий спосіб. Вчиненням кіберзлочинів посадовці, що мають доступ до державних інформаційних систем, спотворюють офіційну функціональність системи держави Україна. В результаті заміщується офіційне призначення держави Україна (гарантування прав та свобод людини) іншим – забезпеченням особистісних інтересів і потреб кіберзлочинців.

Це може бути результатом таких дій:

- несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (стаття 362 ККУ);

- несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації (стаття 362 ККУ).

2. Другий формат проблем системи держави України у зв'язку з вчиненням кіберзлочинів – коли меті не відповідають ні її структура, ні процеси взаємодії окремих частин.

Метою створення та існування системи стверджується: а) певний (заданий ззовні або *встановлений самою системою*) найбільш доцільний (бажаний) кінцевий стан [9, с. 50; 11, с. 85]; б) реалізація необхідного порядку зміни станів (потрібний рух); в) забезпечення потрібного напрямку руху системи без конкретизації кінцевого стану системи [9, с. 50; 20, с. 28–29]. Для штучних систем [9, с. 36] суб'єктивною метою є образи бажаного майбутнього (стану системи або результатів функціонування) [9, с. 38; 20, с. 28–29]. У цьому сенсі метою системи держави Україна є права і свободи людини, які згідно зі ст. 3 Конституції України визначають спрямованість її діяльності.

Структура – це сукупність стійких зв'язків об'єкта, що забезпечують його цілісність і відповідність самому собі, тобто зберігання основних властивостей при різних зовнішніх та внутрішніх змінах, можливість проходження різних видів потоків (матеріальних, енергетичних, інформаційних тощо) [9, с. 32–33]. Структуру системи держави України мають становити владні нормативно скоординовані матеріальні, енергетичні та інформаційні зв'язки. Проте кіберзлочинність ці зв'язки порушує. Вочевидь, у цій частині державна структура процесами взаємодії між суб'єктами проблемно не узгоджується з офіційною метою системи держави Україна, яку було окреслено раніше. Йдеться, зокрема, про порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них

оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію (стаття 363 ККУ).

3. Третім видом проблем недосягнення мети системи держави Україна, передумовою якої є кіберзлочинність, можна вважати неналежну взаємодію цього системного об'єкта зі своїм середовищем: 1)шкідливий вплив зовнішнього середовища на систему; 2)неналежний вплив системи на її зовнішнє середовище.

Відповідно до теорії системотехніки оточенням (зовнішнім середовищем) системи вважається сукупність об'єктів: 1) які впливають на неї; 2) на які вона сама впливає; 3) індиферентні для неї [10, с. 44]. Тож оточенням системи держави України (зовнішнім середовищем) можна стверджувати її населення. Кіберзлочинність впливає на інформаційні процеси, що відбуваються між державою та громадянами, порушуючи їх права і унеможливлюючи досягнення державної мети.

Неналежний вплив держави на оточуюче середовище (громадян-злочинців) у форматі кіберзлочинів відбувається у такий спосіб:

- несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації (стаття 362 ККУ);

- несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства (стаття 361-2 ККУ).

Неналежний вплив зовнішнього середовища (громадян) на систему держави у форматі кіберзлочинів відбувається у такий спосіб:

- несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (стаття 361 ККУ).

- створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (стаття 361-1 ККУ).

- умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (стаття 363-1 ККУ).

Щодо наведеного, принциповим є питання про детермінацію проблем у системі держави України у зв'язку з кіберзлочинністю. Фахівці стверджують, що проблеми у системі формуються через взаємодію декількох класів факторів:

1) чинників різних державних відносин (політичних, економічних, соціальних, етнічних, екологічних та ін.);

2) сил – обставин, за допомогою яких може змінюватися стан вищезгаданих факторів (наука, техніка, технології, культура, релігія та ін.);

3) акторів – людей, організацій, партій, рухів тощо, які маніпулюють силами задля впливу на сили та фактори;

4) цілей акторів, на підставі яких будуються їх мотиваційні дії, що впливають за допомогою сил на фактори;

5) політик акторів – засобів поведінки останніх у процесі досягнення цілей або варіантів і використання ними засобів досягнення мети;

6) системи цінностей, у просторі якої формується проблема.

Такі детермінанти зумовлюють неспівпадіння бажаного (існуючого, очікуваного, обов'язкового) стану речей у системі та результатів її функціонування [8, с. 208]. І з урахуванням цього треба застосовувати заходи вирішення проблеми - заходи запобігання кіберзлочинності.

Висновки і перспективи подальших досліджень. Саме у такому форматі ми вбачаємо формалізацію проблеми кіберзлочинності у системі держави України. У теорії системотехніки стверджується, що вирішити проблему означає перевести проблемо-змістовну систему з проблемного стану у бажаний, тобто в той, коли ліквідуються небажані властивості, а показники критичних властивостей переводяться у прийнятні межі [8, с. 227]. У цьому сенсі формалізація проблеми кіберзлочинності відносно системи держави України методологічно орієнтує заходи превентивної діяльності. При тому заходи запобігання мають враховувати фактори детермінації досліджуваного явища, окреслені вище.

Література

1. Microsoft Digital Defense Report 2024: Microsoft Report. URL: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf (дата звернення: 10.07.2025).

2. Russia's Cyber Tactics: Lessons Learned 2022: Аналітичний звіт Держспецзв'язку про рік повномасштабної кібервійни росії проти України. URL:https://cip.gov.ua/ua/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine (дата звернення: 10.07.2025).

3. Бодунова О. М. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні. *Науковий вісник Ужгородського університету. Серія: Право.* 2023. Т.2, Вип. 75. С. 83-87.

4. Голіна В. В., Лукашевич С. Ю., Колодяжний М. Г. Державне програмування і регіональне планування заходів запобігання злочинності в Україні / за заг. ред. В. В. Голіни. Харків : Право, 2012. 304 с. URL: https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/63.pdf (дата звернення: 10.07.2025).

5. Дунаєва Т. Є. Використання передових технологій у розслідуванні кіберзлочинів. *Використання цифрових технологій у криміналістиці та судовій експертизі : матеріали міжнар. наук.-практ. круглого столу* (м. Харків, 11 груд. 2023 р.). Харків, 2024. С. 71-72. URL: https://ivpz.kh.ua/wp-content/uploads/2024/03/%D0%97%D0%B1%D1%96%D1%80%D0%BA%D0%B0-%D1%82%D0%B5%D0%B7_%D0%92%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F-%D0%A6%D0%A2_2024_%D0%9D%D0%94%D0%86-%D0%92%D0%9F%D0%97-1_compressed.pdf (дата звернення: 10.07.2025).

6. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.2001 р. *Офіційний вісник України*. 2007. № 65. Ст. 2535. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 10.07.2025)

7. Красько М.І., Цевух А.І. Еволюція кіберзлочинності: як кримінальне право адаптується до цифрової ери? *Аналітично-порівняльне*

правознавство. 2025. Вип. 03. Ч.2. С. 387-394. URL: https://scholar.google.com.ua/scholar_url?url=https://app-journal.in.ua/wp-content/uploads/2025/06/APP_03_2025-part-2.pdf%23page%3D387&hl=uk&sa=X&d=15196182336120296125&ei=M99QaPrlLPfWieoPkIfZ2Q8&scisig=AAZF9b90nrpcGfwCUIX4TDyv3WrL&oi=scholaralrt&hist=ZQN_5R8AAAAJ:7526093648855656056:AAZF9b_3pug0HSOJqUVXtbLyvH7L&html=&pos=9&folt=rel&fols= (дата звернення: 10.07.2025).

8. Лямец В. И., Успаленко В. И. Основы общей теории систем и системный анализ : учеб. пособие. Харьков : Бурун и К. ; Киев : КНТ, 2015. 304 с.

9. Лямець В. І., Тевяшев А. Д. Системний аналіз. Вступний курс : монографія. 2-ге вид. Харків : ХНУРЕ, 2004. 448 с.

10. Маца К. А. Системы неорганические, органические, социальные: свойства и принципы организации : монография. Київ : Обрії, 2008. 196 с.

11. Методы исследований и организация экспериментов / под ред. К. П. Власова. Харьков : Гуманитарный Центр, 2002. 256 с.

12. Оболенцев В. Ф. Базові засади системного аналізу злочинності та віктимізації в Україні : монографія. Харків : Юрайт, 2016. 116 с. URL:https://dspace.nlu.edu.ua/bitstream/123456789/12015/1/Obolencev_2016_mon.pdf (дата звернення: 10.07.2025).

13. Оболенцев В. Ф. Системний аналіз та моделювання системи запобігання злочинності в Україні : монографія. Харків : Юрайт, 2021. 192 с. URL: https://dspace.nlu.edu.ua/jspui/bitstream/123456789/19459/1/Obolencev_2021_192.pdf (дата звернення: 10.07.2025).

14. Оболенцев В.Ф. Злочинність як об'єкт криміногенної детермінації в умовах війни рф проти Україні. *Наукові перспективи. Серія "Право".*

2024. № 10(52). С. 948-960. DOI: https://doi.org/10.52058/2708-7530-2024-10(52)-948-960.

15. Оболенцев В.Ф. Механізми детермінації злочинності в умовах російської агресії. *Вісник науки та освіти*. 2024. Вип. 10(28). С. 1607-1617. DOI: https://doi.org/10.52058/2786-6165-2024-10(28)-1607-1617 (дата звернення: 10.07.2025).

16. Оболенцев В.Ф. Моделювання детермінації злочинності. *Актуальні питання у сучасній науці*. 2024. Вип. 11(29). С.629-641. URL: http://perspectives.pp.ua/index.php/sn/article/view/16538/16610 (дата звернення: 10.07.2025).

17. Оболенцев В. Ф. Базові засади системного аналізу системи держави України : монографія. Харків: Право, 2018. 98 с. URL: https://dspace.nlu.edu.ua/bitstream/123456789/17634/1/Obolentsev_2018.pdf (дата звернення: 10.07.2025).

18. Свиридюк Ю. В Україні зафіксували майже 4 000 кібератак з боку РФ. *Суспільне. Новини*. 2023. 18 листопада. URL:https://suspilne.media/619941-v-ukraini-zafiksuvali-majze-4-000-kiberatak-z-boku-rf/ (дата звернення: 10.07.2025).

19. Сорока К. О. Основи теорії систем і системного аналізу : навч. посібник. 2-ге вид. Харків : ФОП Тимченко, 2005. 288 с.

20. Сурмин Ю. П. Теория систем и системный анализ : учеб. пособие. Киев : МАУП, 2003. 368 с.

References

1. Microsoft Digital Defense Report 2024: Microsoft Report. Retrieved from https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf.

2. Russia's Cyber Tactics: Lessons Learned 2022: Analitychnyy zvit Derzhspetszv'yazku pro rik povnomasshtabnoyi kiberviyny rosiyi proty Ukrayiny [Russia's Cyber Tactics: Lessons Learned 2022Analytical report of the State Special Communications Service on the year of Russia's full-scale cyberwar against Ukraine]. (2022). Retrieved from https://cip.gov.ua/ua/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine.

3. Bodunova, O. M. (2023). Zapobihannya zlochynnosti u sferi informatsiynykh tekhnolohiy v umovakh voyennoho stanu v Ukrayini [Prevention of crime in the sphere of information technologies under martial law in Ukraine]. *Naukovyy visnyk Uzhhorods'koho universytetu. Seriya: Pravo – Scientific Bulletin of Uzhgorod University. Series: Law*. Issue 75. Vol. 2. P. 83-87 [in Ukrainian].

4. Holina,V. V., Lukashevych, S. YU., Kolodyazhnyy, M. H. Derzhavne prohramuvannya i rehional′ne planuvannya zakhodiv zapobihannya zlochynnosti v Ukrayini [State programming and regional planning of measures to prevent crime in Ukraine]. Kharkiv: Pravo [in Ukrainian].

5. Dunaeva, T. Ye. (2023). The use of advanced technologies in the investigation of cybercrimes [Vykorystannya peredovykh tekhnolohiy u rozsliduvanni kiberzlochyniv]. *Vykorystannya tsyfrovykh tekhnolohiy u kryminalistytsi ta sudoviy ekspertyzi: materialy mizhnar. nauk.-prakt. kruhloho stolu (m. Kharkiv, 11 hrud. 2023 r.) – The use of digital technologies in forensics and forensic examination: materials of the international scientific-practical round table (Kharkiv, December 11, 2023)*. Kharkiv. P. 71-72. Retrieved from https://ivpz.kh.ua/wp-content/uploads/2024/03/%D0%97%D0%B1%D1%96%D1%80%D0%BA%D0%B0-%D1%82%D0%B5%D0%B7_%D0%92%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F-

%D0%A6%D0%A2_2024_%D0%9D%D0%94%D0%86-%D0%92%D0%9F%D0%97-1_compressed.pdf [in Ukrainian].

6. Konventsiya pro kiberzlochynnist′: Konventsiya Rady Yevropy vid 23.11.2001 r. [Convention on Cybercrime: Council of Europe Convention of 23.11.2001]. (2007). *Ofitsiynyy visnyk Ukrayiny – Official Gazette of Ukraine*, No. 65. Art. 2535 Retrieved from https://zakon.rada.gov.ua/laws/show/994_575#Text [in Ukrainian].

7. Kras′ko M.I., Tsevukh A.I. (2025). Evolyutsiya kiberzlochynnosti: yak kryminal′ne pravo adaptuyet′sya do tsyfrovoyi ery? [The evolution of cybercrime: how is criminal law adapting to the digital era?]. *Analitychno-porivnyal'ne pravoznavstvo – Analytical and comparative jurisprudence*. Vol. 03. Part.2. P. 387-394. Retrieved from https://scholar.google.com.ua/scholar_url?url=https://app-journal.in.ua/wp-content/uploads/2025/06/APP_03_2025-part-2.pdf%23page%3D387&hl=uk&sa=X&d=15196182336120296125&ei=M99QaPrlLPfWieoPkIfZ2Q8&scisig=AAZF9b90nrpcGfwCUIX4TDyv3WrL&oi=scholaralrt&hist=ZQN_5R8AAAAJ:7526093648855656056:AAZF9b_3pug0HSOJqUVXtbLyvH7L&html=&pos=9&folt=rel&fols= [in Ukrainian].

8. Liamets', V.I., Uspalenko, V.I. (2015). Osnovy obshchey teorii sistem i sistemnyy analiz [Fundamentals of general theory of systems and system analysis]. Khar'kov: Burun i K [in Russian].

9. Liamets', V.I., Teviashev, A.D. (2004). Systemnyj analiz. Vstupnyj kurs [Analysis of the systems. Introductory course]. Kharkiv: KhNURE [in Ukrainian].

10. Matsa, K.A. (2008). Systems inorganic, organic, social: properties and principles of organization [Sistemy neorganicheskiye, organicheskiye, sotsial'nyye: svoystva i printsipy organizatsii]. Kyiv: Obriyi [in Russian].

11. Metody issledovaniy i organizatsiya eksperimentov [Methods of research and organization of experiments]. K.P. Vlasov (Ed.). (2002). Khar'kov: Humanitarniy tsentr [in Russian].

12. Obolentsev, V.F. (2015). Bazovi zasady systemnoho analizu zlochynnosti ta victimizatsii v Ukraini [Base principles of analysis of the systems of criminality and victimization in Ukraine]. Kharkiv: Yurait [in Ukrainian].

13. Obolentsev, V. F. (2021). Systemnyy analiz ta modelyuvannya systemy zapobihannya zlochynnosti v Ukrayini [System analysis and modeling of the crime prevention system in Ukraine]. Kharkiv: Yurayt. Retrieved from URL:https://dspace.nlu.edu.ua/jspui/bitstream/123456789/19459/1/Obolencev_2021_192.pdf [in Ukrainian].

14. Obolentsev, V.F. Zlochynnist′ yak ob″yekt kryminohennoyi determinatsiyi v umovakh viyny rf proty Ukrayini [Crime as an object of criminogenic determination in the conditions of the war of the rf against Ukraine.]. *Naukovi perspektyvy. Seriya "Pravo" – Scientific perspectives. Series "Law"*. (Issue 10(52)), (pp. 948-960). https://doi.org/10.52058/2708-7530-2024-10(52)-948-960 [in Ukrainian].

15. Obolentsev, V.F. Mekhanizmy determinatsiyi zlochynnosti v umovakh rosiys′koyi ahresiyi [Mechanisms of crime determination in the conditions of Russian aggression]. *Visnyk nauky ta osvity – Bulletin of Science and Education*. Issue 10(28). P. 1607-1617). https://doi.org/10.52058/2786-6165-2024-10(28)-1607-1617 [in Ukrainian].

16. Obolentsev, V.F. (2024). Modelyuvannya determinatsiyi zlochynnosti [Modeling the determination of crime]. *Aktual'ni pytannya u suchasniy nautsi – Current issues in modern science.* Issue 10(28). P. 629-641. Retrieved from http://perspectives.pp.ua/index.php/sn/article/view/16538/16610 [in Ukrainian].

17. Obolentsev, V.F. (2015). Bazovi zasady systemnoho analizu zlochynnosti ta victimizatsii v Ukraini [Base principles of analysis of the systems of criminality and victimization in Ukraine]. Kharkiv: Yurait. Retrieved from

https://dspace.nlu.edu.ua/bitstream/123456789/17634/1/Obolentsev_2018.pdf [in Ukrainian].

18. Svyrydyuk, Y. (2023). V Ukrayini zafiksuvaly mayzhe 4 000 kiberatak z boku RF [Almost 4,000 cyberattacks from the Russian Federation were recorded in Ukraine]. *Suspil'ne. Novyny. – Social. News*, 18.11. Retrieved from URL:https://suspilne.media/619941-v-ukraini-zafiksuvali-majze-4-000-kiberatak-z-boku-rf/ [in Ukrainian].

19. Soroka, K.O. (2005). Osnovy teorii system i systemnoho analizu [Bases of theory of the systems and analysis of the systems]. Kharkiv: FOP Tymchenko [in Ukrainian].

20. Surmin, Y. P. Teoriya sistem i sistemnyy analiz [Theory of systems and system analysis]. Kiyev : MAUP [in Ukrainian].