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

DOI: 10.25313/2520-2308-2025-7-11244

СИСТЕМА ЗАХОДІВ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

SYSTEM OF CYBERCRIME PREVENTION MEASURES

Анотація. *Вступ. У зв'язку з досягненнями науково-технічного прогресу цифровізація суспільних відносин стає цивілізаційним трендом. Одночасно поширюється й пов'язана з нею кіберзлочинність, яка негативно впливає на різні сфери життєдіяльності людей. В Україні кіберзлочини є вагомою складовою російської агресії. За таких обставин розробка дієвої теорії заходів запобігання кримінальним правопорушенням у сфері інформаційних технологій набуває для українського суспільства особливої актуальності.*

Мета. Метою статті визначено формулювання системних властивостей та класифікаційних характеристик системи заходів запобігання кібезлочинів.

Матеріали і методи. У дослідженні використано: 1) нормативно-правові акти; 2) результати наукових досліджень щодо заходів запобігання кіберзлочинності. Використані методи: теоретичного узагальнення (для характеристики напрацювань науковців за досліджуваною тематикою); класифікації (для встановлення класифікаційних характеристик досліджуваної сфери правоохоронної діяльності); логічного синтезу (для формулювання висновків роботи); методику системного аналізу (для формалізації мети, призначення та функцій системи запобігання кіберзлочинності).

Результати. В роботі визначено мету системи запобігання кіберзлочинності – відсутність кримінально караних порушень існуючих суспільних відносин у сфері використання інформаційних технологій.

Призначенням системи запобігання кіберзлочинності стверджується утримання населення від порушення правомірних суспільних відносин, перешкоджання потенційній або розпочатій злочинній діяльності у цій сфері.

Функціями досліджуваної системи окреслено способи утримання населення від злочинних дій та припинення розпочатих злочинних посягань у сфері використання інформаційних технологій. Фактично це спеціально-кримінологічні та індивідуальні заходи запобігання.

Система запобігання кіберзлочинності є штучною відкритою нелінійною складною багатофункціональною імовірнісною скелетною дискретною поведінковою цілеспрямованою «добре організованою» макросистемою, що знаходиться на стадії «зрілості».

Перспективи. Наведені системні характеристики мети, призначення та функцій системи запобігання кіберзлочинності, а також її класифікаційні характеристики мають стати підґрунтям для подальших напрацювань щодо системи запобігання правопорушень у сфері інформаційних технологій. Ці обставини треба враховувати у подальших дослідженнях та у нормотворчості.

Ключові слова: *кіберзлочинність, кіберзлочини, система запобігання кіберзлочинності.*

Summary. *Introduction. Due to the achievements of scientific and technological progress, the digitalization of social relations is becoming a civilizational trend. At the same time, cybercrime, which is associated with it, is spreading, which negatively affects various spheres of people's lives. In Ukraine, cybercrime is a significant component of Russian aggression. Under such circumstances, the development of an effective theory of measures to prevent criminal offenses in the field of information technologies becomes particularly relevant for Ukrainian society.*

Purpose. The article aims to formulate the systemic properties and classification characteristics of the system of measures to prevent cybercrime.

Materials and methods. The study used: 1) regulatory and legal acts; 2) results of scientific research on measures to prevent cybercrime. The methods used were: theoretical generalization (to characterize the work of scientists on the topic under study); classification (to establish classification characteristics of the studied area of law enforcement activity); logical synthesis (to formulate conclusions of the work); system analysis methodology (to formalize the purpose, purpose and functions of the cybercrime prevention system).

Results. The work defines the goal of the cybercrime prevention system – the absence of criminally punishable violations of existing social relations in the field of information technology use.

The purpose of the cybercrime prevention system is to deter the population from violating legitimate social relations and to prevent potential or initiated criminal activity in this area.

The functions of the studied system outline ways to deter the population from criminal acts and stop initiated criminal attacks in the field of information technology use. In fact, these are special criminological and individual prevention measures.

The cybercrime prevention system is an artificial open nonlinear complex multifunctional probabilistic skeletal discrete behavioral purposeful "well-organized" macrosystem that is at the stage of "maturity".

Discussion. The above systemic characteristics of the purpose, purpose and functions of the cybercrime prevention system, as well as its classification characteristics, should become the basis for further developments regarding the system for preventing offenses in the field of information technology. These circumstances should be taken into account in further research and in rulemaking.

Key words: *cybercrime, cybercrimes, cybercrime prevention system.*

Постановка проблеми. Наскільки цифровізація стає цивілізаційним трендом, наскільки ж пов'язана з нею кіберзлочинність обґрунтовано вважається явищем, як негативно впливає на різні сфери життєдіяльності світової спільноти [1]. Особливо наочно це проявляється в Україні, де кіберзлочини є вагомою часткою російської агресії [2; 19].

За таких обставин розробка дієвої теорії заходів запобігання кримінальним правопорушенням у сфері інформаційних технологій набуває для українського суспільства виняткової актуальності.

Аналіз останніх досліджень і публікацій. Узагальнення напрацювань вітчизняних фахівців щодо теорії та практики запобігання кіберзлочинів дає підстави виділити, зокрема, три їх ґрунтовні напрямки.

1. Теорія використання спеціальних криміналістичних методик для розслідування кіберзлочинів (наприклад, Дунаєва Т. Є.[5]).

2. Дослідження ефективності кримінально-правових заходів у протидії кіберзлочинам (наприклад, Красько М.І, Цевух А. І. [7]).

3. Запобігання кіберзлочинів в умовах воєнного стану в Україні (наприклад, Бодунова О. М. [3]).

4. Запобігання окремих видів кіберзлочинів (наприклад, Малетов Д. В., Печена Т. О. [10]).

На нашу ж думку, перспективним концептуальним напрямком у розробці теорії заходів запобігання кіберзлочинів мають стати напрацювання на засадах теорії системотехніки [8, 14; 15; 16; 17].

Мета статті. Відповідно до окресленої проблематики метою статті визначено формулювання системних властивостей та класифікаційних характеристик системи заходів запобігання кібезлочинів.

Матеріали і методи. В якості матеріалів дослідження використано: 1) нормативно-правові акти щодо заходів запобігання кіберзлочинів; 2) наукові публікації щодо заходів запобігання кіберзлочинності.

Для характеристики напрацювань науковців за досліджуваною тематикою було використано науковий метод теоретичного узагальнення. Метод аналізу документів застосовано щодо дослідження нормативних першоджерел. Методику системного аналізу використано для формалізації мети, призначення та функцій системи запобігання кіберзлочинності. За допомогою методу класифікації встановлено класифікаційні характеристики досліджуваної сфери правоохоронної діяльності, а за допомогою методу логічного синтезу сформульовано висновки роботи.

Викладення основного матеріалу. Мета системи визначається як результат її функціонування, до якого вона прагне на певному етапі свого життєвого циклу [9]. Загальну теорію мети системи запобігання злочинності нами було розглянуто у [14]. З урахуванням цього мету системи запобігання кіберзлочинності як штучної системи можна визначити у такому варіанті: відсутність кримінально караних порушень існуючих суспільних відносин у сфері використання інформаційних технологій. Така діяльність забезпечує права громадян, що є метою системи держави України відповідно до ч. 2 ст. 3 Конституції України.

Призначенням системи запобігання кіберзлочинності (декларована здатність виконати функції, що забезпечують досягнення її мети[9]) збігається з аналогічною характеристикою системи запобігання злочинності в Україні[14], але проявляється щодо сфери використання інформаційних технологій. Фактично йдеться про утримання населення від порушення правомірних суспільних відносин, перешкоджання потенційній або розпочатій злочинній діяльності у цій сфері.

Відповідно до теорії систем функції об'єкта ототожнюють із здатністю до дії; впливом; задоволенням потреб; роллю; обов'язками, перетворенням призначення системи на дії[9]. Для системи запобігання кіберзлочинності функціями можна вважати способи утримання населення від злочинних дій та припинення розпочатих злочинних посягань у сфері використання інформаційних технологій.

З урахуванням теорії кримінології можна стверджувати, що функції системи запобігання кіберзлочинності — це спеціально-кримінологічні та індивідуальні заходи її запобігання [4].

Класифікація — це розподіл елементів на групи відповідно до обраних критеріїв. Застосування цього наукового методу допомагає порівняти однорідні об'єкти та з'ясувати їх сутнісні характеристики. Теорія цього засобу пізнання розроблена у теорії логіки і плідно використовується у системному аналізі [9, с. 24, 26]. Власні ж дослідження за цією науковою методикою окреслили важливу інформацію щодо характеристик системи запобігання кіберзлочинності.

За наявністю матеріального субстрату системи (об'єкти) поділяють на матеріальні (об'єкти з матеріальними елементами) та ідеальні (ті, що не мають матеріального субстрату — системи понять, інші логічні конструкції)[11, с. 74]. Система запобігання кіберзлочинності (правоохоронних органів) являє собою зкоординовану діяльність людей, тож це система матеріальна. Відповідно, в ній проявляються закономірності матеріального Світу що суттєво визначають її функціональність.

Наведену класифікацію прийнято додатково уточнювати за критерієм типу матеріального субстрату, з якого створені системи. При тому виділяють неорганічні системи (планети, атмосфера), органічні (популяції живих істот), соціальні системи (людські осередки), змішані (галузі економіки, домогосподарства) [11, с. 76]. У цій класифікації система запобігання кіберзлочинності являє собою клас соціальних систем, що функціонує за соціальними закономірностями.

За походженням елементів виділяють системи природні, штучні та змішані. Природні — це ті, які створені і функціонують як складові природнього Світу (мікроорганізми, популяції тварин). Штучні системи створюються людиною (технічні об'єкти, соціальні осередки). Комбіновані системи мають властивості і природніх, і штучних систем (зоопарк, штучні водоймища) [11, с. 75]. Відповідно до цієї класифікації систему запобігання кіберзлочинності є штучною системою, адже її створили люди, уповноважені керувати правоохоронною діяльністю. Для штучних систем перед їх безпосереднім створенням визначаються суб'єктивні цілі, на досягнення яких спрямовується системна функціональність. [9, с. 38; 20, с. 28–29].

За ознакою ступеня відкритості виділяють системи закриті, які не обмінюються з оточуючим середовищем матерією, енергією та інформацією, та відкриті, в яких наявні процеси такого обміну. Оскільки система запобігання кіберзлочинності обмінюється з суспільством, зокрема, інформацією, тож вона є системою відкритою. У теорії систем стверджується, що відкритість, тобто взаємодія із оточуючим середовищем дозволяє системам забезпечувати себе ресурсами у досягненні своєї мети. Принциповим є також те, що відкриті системи можуть самоналаштовуватися відповідно до впливу зовнішнього середовища. Вочевидь ця обставина є принциповою для системи запобігання кіберзлочинності як складового елементу загальної системи охорони прав громадян.

Важливою складовою у функціонуванні систем є їх керування. Для його розуміння системи класифікують на ступенем однорідності елементів на лінійні та нелінійні. Лінійні системи складаються з однорідних елементів (шкільні класи), а нелінійні — з різнорідних (галузі виробництва). Враховуючи наявність різних структурних підрозділів, система запобігання кіберзлочинності являє собою систему нелінійну. Обґрунтовано вважається, що управління нелінійними системами є більш складним завданням, ніж управління системами лінійними (простими). Цю обставину треба враховувати у нормотворчості, яка формує основи функціоналу досліджуваної сфери правоохоронної діяльності.

Системи поділяють на види з урахуванням ступеня складності. Критерієм такої класифікації є кількість та складність їх елементів та підсистем, тип внутрішніх та зовнішніх взаємозв'язків між елементами, тип зв'язків, кількість та складність функцій, що виконують системи. Відповідно щодо цього виділяють системи прості (до 10^3 елементів), складні системи (до 10^9 елементів), надскладні системи (до 10^9 елементів). Відповідно до окресленого система запобігання кіберзлочинності є складною системою. Щодо цього виду систем науковці стверджують про функціональну інерційність у протидії впливу зовнішнього середовища. Пояснюється це тим, що збільшення кількості складових елементів збільшує й здатність їх взаємозаміни, підвищуючи стійкість системних об'єктів в цілому.

Щодо згаданого аспекту принциповою є також й класифікація систем за фізичними параметрами розмірів, довжини та обсягу: мікросистеми, мезосистеми; макросистеми; метасистеми, мегасистеми (Всесвіт) [11, с. 77]. У цій класифікації система запобігання кіберзлочинності є макросистемою. Обґрунтовано вважається, що системи малого масштабу не можуть бути стійкими, оскільки на них постійно впливає зовнішнє середовище. І навпаки, великі системи є більш стійкими.

За кількістю функцій системи поділяють на одно– та багатофункціональні. Вище нами було розкрито функції системи запобіганні кіберзлочинності — способи утримання населення від злочинних дій

та припинення розпочатих злочинних посягань (спеціально-кримінологічні та індивідуальні заходи запобігання злочинності) [4, с. 47]. Це доволі різні види діяльності за суб'єктами та змістом, тож систему запобігання кіберзлочинності маємо стверджувати як багатофункціональну систему. І цю обставину треба враховувати у нормотворчості щодо досліджуваної сфери.

За передбачуваністю результату функціонування у теорії системотехніки виділяють системи детерміновані та ймовірнісні. Перший вид — детерміновані системи — для них кінцевий результат функціонування заздалегідь визначений проектувальниками або передбачуваний. Навпаки, в імовірнісних системах кінцевий результат функціонування передбачити заздалегідь неможливо [11, с. 79]. Система запобігання кіберзлочинності опрацьовує великий обсяг неочевидної інформації щодо латентних кримінальних правопорушень, тому результат діяльності її складових елементів у цілому передбачити неможливо. Тож систему запобігання кіберзлочинності маємо вважати імовірнісною системою, для якої передбачення результатів функціонування ускладнено [11, с. 79].

Системи поділяють залежно від особливостей їх структури. Перший вид — це так звані центристські системи, в яких організуючі елементи знаходяться у центрі (такою є, наприклад, Сонячна система). Другий вид — скелетні, у яких організуючі елементи розташовані по осі (дерева). У третьому типі — сотовому, організуючі елементи розташовані по всій системі[11, с. 78]. Систему запобігання кіберзлочинності належить до класу скелетних систем, адже вона організована у форматі ієрархічної вертикалі суб'єктів управління та підпорядкованих підрозділів — від вищих органів державної влади до виконавців, працівників відомчих підрозділів.

За просторовим розташуванням системи поділяють на континуальні суцільні (море, атмосфера) та дискретні несуцільні (ліс) системи. Відповідно, у цій класифікації система запобігання кіберзлочинності належить до дискретних систем. Це треба враховувати при розгляді її структурних зв'язків.

Системи вирізняються за стадіями розвитку — виникнення, становлення, зрілість, криза, перетворення. Вбачається, що система запобігання кіберзлочинності в Україні знаходяться на стадії «зрілості». Для неї є характерним сформованість основних функціоналів та їх належна ефективність.

Серед систем за ознакою поведінкових характеристик виділяють реактивні та поведінкові. Реактивні системи на вплив зовнішнього середовища реагують пасивно, а поведінкові — активно. Система запобігання кіберзлочинності в різний спосіб реагує на прояви зовнішнього середовища (кіберзлочини), тож є системою поведінковою.

Поведінкові системи поділяють на системи адаптивні та системи цілеспрямовані. Адаптивні реагують на вплив зовнішнього середовища несвідомо (наприклад, рослини). Цілеспрямовані реагують на вплив зовнішнього середовища свідомо у процесі виконання своїх функцій. Саме так функціонує система запобігання кіберзлочинності як цілеспрямована система. Таку обставину треба враховувати під час визначення механізмів досягнення системної мети.

Серед систем виділяють «добре організовані системи» та «погано організовані системи». Щодо «добре організованих систем» є можливість визначити всі компоненти та зв'язки, навіть описати їх формулами чи рівняннями[9, с. 40–41]. У випадках визначення об'єкта як «погано організованої системи» завдання визначення всіх компонентів та зв'язків між ними не ставиться. Система описується певним набором мікропараметрів та закономірностями, що встановлюються дослідженням не об'єкта у цілому, а виділенням та розглядом певної їх частини (вибіркової сукупності). І вже потім результати дослідження цієї вибіркової сукупності переносяться на всю систему з певною ймовірністю [9, с. 41]. Враховуючи суттєві обсяги нормативного регулювання досліджуваної сфери та наявну відомчу звітність, систему запобігання кіберзлочинності можна визначити як таку, що належить до класу «добре організованих систем».

Висновки і перспективи подальших досліджень. Наведений матеріал окреслює системні властивості запобігання кіберзлочинності — мету, призначення, функції. Принциповим також є розуміння цього явища як матеріальної соціальної штучної відкритої нелінійної складної багатофункціональної імовірнісної скелетної дискретної поведінкової цілеспрямованої «добре організованої» макросистеми, що знаходиться на стадії «зрілості». Ці обставини мають бути враховані у подальших дослідженнях та у нормотворчості щодо заходів запобігання кіберзлочинів.

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. Лямець В.И., Успаленко В.И. Основы общей теории систем и системный анализ: учеб. пособие. Харьков : БУРУН и К., 2015. 304 с.

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

10. Малетов Д.В., Печена Т.О. Запобігання кіберзлочинам за допомогою додатку «Дія». *Реформування правової системи в контексті євроінтеграційних процесів: матеріали VI Міжнародної науково-практичної конференції,* м. Суми, 19–20 травня 2022 р. Суми: Сумський державний університет, 2022. С. 455–460.

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

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

13. 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)

14. Оболенцев В.Ф. Системний аналіз та моделювання системи запобігання злочинності в Україні. 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).

15. Оболенцев В.Ф. Злочинність як об'єкт криміногенної детермінації в умовах війни РФ проти Україні. *Наукові перспективи. Серія «Право».* 2024. No 10(52). С. 948–960. DOI: https://doi.org/10.52058/2708-7530-2024-10(52)-948-960

16. 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

17. 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)

18. 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).

19. 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).

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

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, 2024. P. 71–72. Retrieved from 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 [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 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= [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. Maletov D.V., Pechena T.O. (2022) Zapobihannya kiberzlochynam za dopomohoyu dodatku "Diya" [Preventing cybercrime using the "Diya" application]. Reformuvannya pravovoyi systemy v konteksti yevrointehratsiynykh protsesiv: materialy VI Mizhnarodnoyi naukovo-praktychnoyi konferentsiyi (Sumy, 19–20 travnya 2022 r.) S. 455–460. — Reforming the legal system in the context of European integration processes: proceedings of the VI International Scientific and Practical Conference (Sumy, May 19–20). Pp. 455–460 [in Ukrainian].

11. 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].

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

13. 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].

14. 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 [in Ukrainian].

15. 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). DOI: https://doi.org/10.52058/2708-7530-2024-10(52)-948-960 [in Ukrainian].

16. 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). DOI: https://doi.org/10.52058/2786-6165-2024-10(28)-1607-1617 [in Ukrainian].

17. 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].

18. 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].

19. Svyrydyuk, YU. (2023). V Ukrayini zafiksuvaly mayzhe 4000 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].

20. 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].