SECTION 5. PUBLIC LAW, SECURITY, AND DIGITALIZATION OF THE STATE

DOI https://doi.org/10.30525/978-9934-26-629-4-17

АДМІНІСТРАТИВНО-ПРАВОВІ МЕХАНІЗМИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ВИКОРИСТАННЮ ШКІДЛИВИХ ПРОГРАМНИХ ПРОДУКТІВ, ЯКІ СТАНОВЛЯТЬ ЗАГРОЗУ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ: ДОКТРИНА ТА СТРАТЕГІЯ ПОВОЄННОГО ВІДНОВЛЕННЯ

Євдокименко Д. М.

ВСТУП

Сучасний світовий порядок демонструє наростання геополітичної напруженості, яка виливається у конфлікти нового типу. Ці протистояння виходять далеко за межі традиційного розуміння війни, адже в них гібридно поєднуються військові, економічні, інформаційні та кібернетичні інструменти впливу. В такій реальності цифровий простір перетворився на стратегічне середовище, де розгортаються операції з дестабілізації держав та маніпулювання суспільною свідомістю. Фактично, кіберпростір став повноцінним «театром воєнних дій», де боротьба ведеться не стільки за території, скільки за контроль над даними і технологіями. Програмне забезпечення (ПЗ) зазнало так званої «вепонізації», перетворившись з об'єкта на інструмент агресії, який використовується для атак на критичну інфраструктуру, шпигунства та поширення дезінформації. Звіт Світового економічного форуму «Global Cybersecurity Outlook 2025» цілком слушно вказує на вразливості в ланцюгах постачання та геополітичну напруженість як на ключові фактори ризику[1].

Для України, яка щоденно зазнає кібератрегресії з боку російської федерації, ця проблема є особливо гострою. Водночас її вирішення лежить у глобальному руслі. Так, ініційований ООН «Глобальний цифровий договір» в рамках «Пакту в ім'я майбутнього» ставить за мету формування «безпечного і надійного цифрового майбутнього для всіх»[1]. Це свідчить про те, що розробка національних превентивних

[1] Pact for the Future : resolution adopted by the General Assembly on 22 September 2024. A/RES/79/1. URL: https://documents.un.org/doc/undoc/gen/N24/164/33/pdf/N2416433.pdf (дата звернення: 29.10.2025).

механізмів є не лише вимушеною відповіддю на агресію, а й кроком до реалізації передових міжнародних стандартів. Залежність економіки та державного управління від іноземного ПЗ актуалізує поняття цифрового суверенітету як ключового елемента національної стійкості. Використання програм, контрольованих державою-агресором, перетворює об'єкти критичної інфраструктури (ОКІ) на плацдарми для диверсій. Тому питання контролю за обігом такого ПЗ виходить за межі суто технічних аспектів і переходить у площину стратегічного адміністративно-правового регулювання.

Ця залежність є не просто теоретичною, вона створює конкретні довгострокові ризики. Йдеться про так званий «вендорний замок» (vendor lock-in) – ситуацію, коли державні інституції та цілі галузі економіки стають настільки інтегрованими з певним програмним продуктом, що перехід на альтернативні рішення стає надзвичайно дорогим та складним з технічної точки зору. Держава-агресор, усвідомлюючи це, може роками не використовувати закладені вразливості, утримуючи «цифровий важіль» впливу, щоб активувати його у найбільш кризовий для країни момент. Чи може держава дозволити собі таку стратегічну вразливість, особливо в контексті повоєнного відновлення, яке саме по собі вимагатиме максимальної стійкості?

Згідно зі звітом Національної поліції України за 2024 рік, значна частина правопорушень у воєнний час пов'язана з «використанням шахраями емоційного стану громадян»[2], що часто реалізується через шкідливе ПЗ. Глобальні ж збитки від кіберзлочинів, за даними ФБР, сягнули 12,5 мільярдів доларів[3]. Проте домінуюча в Україні модель протидії залишається реактивною, кримінально-правовою. Вона фокусується на кваліфікації вже вчинених злочинів (ст. 361, 361-1 КК України[4]), що є запізнілою реакцією. Фундаментальна вада такого підходу криється в асиметрії між швидкістю цифрових атак та повільним темпом кримінального провадження. Атака триває хвилини, а розслідування – місяці. Це робить кримінальну юстицію інструментом постфактум-констатації, а не запобігання шкоді.

[2] Звіт про результати роботи у 2024 році / Національна поліція України. Київ, 2025. 18 с. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2024/zvit-npu-2024.pdf (дата звернення: 20.10.2025).

[3] Internet Crime Report 2024 / Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). 2025. 47 p. URL: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf (дата звернення: 20.10.2025).

[4] Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. *Відомості Верховної Ради України.* 2001. № 25–26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 20.10.2025).

Більше того, кримінально-правове реагування за своєю суттю є індивідуалізованим – воно спрямоване на конкретного виконавця злочину. Проте в умовах гібридної війни програмні загрози часто є не результатом дій окремого хакера, а продуктом діяльності цілих інституцій держави-агресора, її спеціальних служб та афілійованих компаній. Спроба застосувати інструментарій, розрахований на індивідуальну відповідальність, до системного, інституціоналізованого явища апріорі є малоефективною. Це ставить перед правовою наукою фундаментальне питання: чи здатні класичні інститути права адекватно реагувати на загрози, що мають державний масштаб та технологічний характер?

Актуальність цього дослідження зумовлена саме відсутністю дієвих превентивних інструментів. Метою роботи є наукове обґрунтування потреби у формуванні цілісної системи адміністративно-правової превенції програмних загроз та розробка її моделі як передумови для повоєнного відновлення.

1. Парадигмальний зсув від реактивної кримінальної юстиції до проактивного управління кіберризиками

Фундаментальна розбіжність між кримінально-правовим та адміністративно-правовим підходами криється в самому об’єкті захисту. Кримінальне право ретроспективне: воно карає винного за вже вчинене суспільно небезпечне діяння. Натомість логіка адміністративного права, особливо у сфері безпеки, є проспективною, превентивною – воно спрямоване на управління ризиками для захисту правопорядку від потенційних загроз. Саме ця відмінність зумовлює необхідність зміни парадигми.

Правовою основою для такого превентивного втручання є позитивний обов’язок держави щодо захисту національної безпеки та забезпечення стабільного функціонування суспільних інститутів. На відміну від кримінального права, де підставою є склад кримінального правопорушення, в адміністративному праві підставою для примусу може бути реальна загроза настання шкідливих наслідків. Це дозволяє державі діяти на випередження.

Такий проактивний підхід не є винаходом сьогодення; він є іманентною властивістю адміністративного права, що реалізується, наприклад, у сферах санітарного контролю, пожежної безпеки чи ядерного регулювання. Держава не чекає на епідемію, щоб заборонити продаж небезпечних продуктів, і не чекає на пожежу, щоб вимагати встановлення протипожежних систем. Аналогічно, у цифровій сфері очікування реалізації кібератаки для того, щоб вжити заходів щодо небезпечного ПЗ, є формою інституційної бездіяльності. Йдеться

про поширення вже існуючої та апробованої логіки превентивного державного нагляду на нову, цифрову сферу суспільних відносин.

Класичний кримінально-правовий підхід до кіберзлочинів в умовах гібридної війни стикається з низкою практично нездоланних викликів. Це, по-перше, виклик атрибуції – встановлення кінцевого виконавця атаки, прихованого за ланцюгом проксі-серверів та спонсорованих державою-агресором хакерських груп. По-друге, це проблема доказування умислу у розробника ПЗ подвійного призначення. По-третє, це юрисдикційні колізії, коли учасники атаки перебувають у різних країнах.

По суті, ми спостерігаємо конфлікт темпоральностей: швидкість та плинність цифрових загроз протиставляється розмірeності та формалізованості кримінального процесу. Кримінальний закон ефективний там, де є дискретний, завершений акт правопорушення. Програмна загроза, навпаки, є триваючим процесом, латентною вразливістю, яка може існувати роками, перш ніж буде активована. Намагатися застосувати до цього процесу норми, розраховані на фіксацію події злочину, – це все одно, що грати в шахи за правилами з минулого століття проти супротивника, який використовує квантові обчислення. Система права має адаптуватися, інакше вона ризикує перетворитися на архаїчний механізм, нездатний захистити суспільство.

Особливо гостро ця проблема проявляється у випадку так званих Advanced Persistent Threats (APTs) – складних, цілеспрямованих та тривалих кібератак, за якими, як правило, стоять державні «виконавці». Такі групи діють під прикриттям доктрини «правдоподібної заперечуваності» (plausible deniability), використовуючи складну інфраструктуру та формально не пов’язаних з урядом виконавців. Довести в рамках кримінального процесу зв’язок між конкретною кібератакою та урядовими структурами іншої держави – завдання, що межує з неможливістю. Це створює «вікно безкарності», в якому агресор може діяти практично без ризику юридичної відповідальності.

Ці виклики фактично нівелюють превентивний потенціал кримінального переслідування. Наслідком є стан перманентної вразливості, за якого держава завжди наздоганяє. Агресор, використовуючи переваги цифрового простору, може досягати своїх цілей з низьким ризиком відповідальності. Шкода вже завдана, а можливості для її компенсації обмежені. Саме тому превенція на основі адміністративно-правових інструментів стає єдиноможливою стратегією для відновлення паритету. Не дивно, що передові міжнародні практики, як-от “Cybersecurity Handbook” Греції, акцентують увагу на

ешелонованих системах захисту, де адміністративні заходи відіграють першочергову роль[5].

Це вимагає переосмислення об'єкта регулювання. Замість вузького поняття «шкідливе ПЗ» (malware), доцільно запровадити ширшу доктринальну категорію – «програмне забезпечення, що становить загрозу національній безпеці». Вона має охоплювати будь-які програмні продукти, що створюють неприйнятний ризик, зокрема:

1) ПЗ, афілійоване з державою-агресором, розробники чи бенефіціари якого пов'язані з рф (напр., Kaspersky, 1C, Bitrix24).

2) ПЗ подвійного призначення, що активно використовується у кібератаках, на що вказує і звіт Europol IOCTA 2024[6].

3) ПЗ, що здійснює надлишковий збір даних та передає їх на сервери у ризикових юрисдикціях.

Запропоновану категорію можна структурувати за типами ризиків: порушення конфіденційності даних (шпигунство), порушення доступності сервісів (можливість дистанційного відключення) та інформаційно-когнітивні ризики (поширення дезінформації). Комплексний аналіз ПЗ має враховувати всі три виміри. Ключова перевага такого підходу – зміна підстав для втручання держави. Замість доведення суб'єктивного умислу особи, держава обґрунтовує свої дії на основі об'єктивної оцінки небезпеки самого продукту.

Варто окремо зупинитися на правовій дилемі, яку створює ПЗ подвійного призначення. З юридичної точки зору, інструмент для віддаленого адміністрування є аналогом слюсарного інструменту: сам по собі він легальний і може використовуватися як для законних цілей (ремонт), так і для незаконних (злам замка). Оскільки об'єктивна сторона (розробка та розповсюдження такого ПЗ) є правомірною, єдиною підставою для кримінальної відповідальності може бути доведення суб'єктивної сторони – злочинного умислу розробника. Однак довести, що продукт створювався саме з метою його подальшого неправомірного використання, без прямого зізнання чи внутрішньої документації компанії практично неможливо. Адміністративний підхід, натомість, дозволяє оминути цю проблему, оцінюючи не умисел розробника, а об'єктивні ризики, які створює широке та не контрольоване розповсюдження такого «універсального інструменту».

[5] Cybersecurity Handbook: Best Practices for the Protection and Resilience of Network and Information Systems / Hellenic Republic, Ministry of Digital Governance, National Cybersecurity Authority. June 2021. 76 p. URL: https://cyber.gov.gr/wp-content/uploads/2025/03/Cybersecurity-Handbook-English-version-compressed.pdf (дата звернення: 20.10.2025).

[6] Internet Organised Crime Threat Assessment (IOCTA) 2024 / Europol. 2024. 76 p. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf (дата звернення: 20.10.2025).

2. Концептуальна модель адміністративно-правового механізму превенції програмних загроз

Формування дієвої превентивної системи вимагає побудови чіткого та інституційно забезпеченого механізму. Його архітектура має спиратися на міжнародний досвід (напр., американський «Entity List»[7], європейська NIS2 Directive[8]), але враховувати українську специфіку. Пропонується модель, що складається з трьох елементів.

Хоча запропонована модель спирається на такі відомі аналоги, як американський «Entity List» чи європейські підходи в рамках Директиви NIS2, вона має принципову відмінність. Якщо «Entity List» є переважно інструментом зовнішньоекономічної та санкційної політики, спрямованим на обмеження доступу певних компаній до американських технологій, то запропонований український механізм є інструментом внутрішнього адміністративного ризик-менеджменту. Його першочергова мета – не покарати іноземного виробника, а захистити власну національну інфраструктуру від потенційно небезпечного продукту, незалежно від наявності формальних міжнародних санкцій. Цей акцент на внутрішній превенції є ключовим.

1) Ядро механізму – уповноважений суб'єкт та методологія оцінки ризиків. Необхідно законодавчо визначити такий орган. Оптимальним видається створення постійно діючої міжвідомчої комісії при РНБО, що відповідатиме стратегічним напрямам державної політики у цій сфері[9], куди увійдуть фахівці СБУ, Держспецзв'язку, розвідки, НКЦК, Кіберполіції та незалежні експерти. Саме міжвідомчий характер дозволить синтезувати технічну, оперативно-розшукову та правову експертизу. Цей орган має розробити та публічно затвердити Методику оцінки ризиків ПЗ за сукупністю критеріїв: технічних, геополітичних, юридичних та репутаційних. Такий інклюзивний підхід, що відповідає принципам «Глобального цифрового договору», є запорукою легітимності рішень. Важливим аспектом є запобігання регуляторній

[7] Where can I find the Entity List? / U.S. Department of Commerce, Bureau of Industry and Security. URL: https://www.bis.doc.gov/index.php/component/fsj_faqs/faq/106-where-can-i-find-the-entity-lis (дата звернення: 20.10.2025).

[8] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union. 27.12.2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02022L2555-20221227 (дата звернення: 20.10.2025).

[9] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» : Указ Президента України від 26.08.2021 р. № 447/2021. *Офіційний вісник України.* 2021. № 68. Ст. 4295. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 20.10.2025).

упередженості. Залучення незалежних експертів дозволить збалансувати інтереси безпеки з потребами економіки, уникнувши надмірного тиску на ринок.

Діяльність такої комісії має бути чітко регламентована на законодавчому рівні, аби уникнути ризиків перевищення повноважень чи політичного тиску. Регламент її роботи повинен передбачати кворум, порядок голосування, а головне – обов'язок мотивувати кожне своє рішення. Мотивувальна частина рішення про внесення ПЗ до реєстру повинна містити детальний аналіз ризиків за затвердженою методикою, з посиланням на конкретні факти, технічні звіти або дані розвідки. Саме обґрунтованість рішення є запорукою його стійкості під час потенційного судового оскарження.

2) Інструмент реалізації – публічний реєстр небезпечного ПЗ. Рішення комісії має фіксуватися шляхом внесення ПЗ до відкритого реєстру. З правової точки зору, це не просто інформаційний ресурс, а інструмент політики. Включення до реєстру є адміністративним актом, що породжує правові наслідки. Такий реєстр виконує функцію створення юридичної визначеності. Суб'єкти господарювання отримують чітке джерело інформації про статус програм, що дозволяє заздалегідь планувати діяльність та уникати ризиків. Окрім опису загроз та правового режиму, реєстр має містити перелік рекомендованих безпечних аналогів.

3) Способи впливу – диференційовані правові режими. Залежно від рівня загрози, для ПЗ встановлюються такі режими:

– режим заборони («червоний» рівень): повна заборона використання в органах влади та на об'єктах критичної інфраструктури (ОКІ);

– режим обмеження («помаранчевий» рівень): дозвіл на використання за певних умов (напр., в ізольованому середовищі);

– режим інформування («жовтий» рівень): для приватного сектору та громадян. Держава офіційно попереджає про ризики, що в разі настання шкоди може вплинути на питання відповідальності та страхового відшкодування.

В основі такого підходу лежить принцип пропорційності: заходи мають бути адекватними загрозі. Заборона – це крайній захід (ultima ratio) для найвищих ризиків. Для гарантування прав виробників рішення про внесення до реєстру має ухвалюватися за чіткою адміністративною процедурою, що включає право на пояснення та механізм судового оскарження. Особливої уваги потребують саме процедурні гарантії. Оскільки внесення до реєстру є позасудовим обмеженням прав, воно має бути обґрунтованим та оскаржуваним, аби

відповідати критеріям правової держави та уникнути зловживань. Важливо наголосити, що модель має бути динамічною. Цифрове середовище змінюється, тому необхідно передбачити процедури періодичного перегляду статусу ПЗ в реєстрі, а також механізм його виключення, якщо ризики усунуто.

Важливим є і питання повноти судового контролю за рішеннями комісії. Суд, розглядаючи відповідні спори, не повинен перебирати на себе невластиву йому функцію технічного експерта та самостійно оцінювати рівень кіберзагрози. Його завдання – перевірити, чи діяла комісія в межах своїх повноважень, чи було її рішення ухвалене на підставі належних доказів, з дотриманням встановленої процедури, та чи є застосований обмежувальний режим пропорційним доведеним ризикам. Саме такий підхід, що фокусується на дотриманні процедури, обґрунтованості та пропорційності, відповідає найкращим практикам адміністративної юстиції у справах, що стосуються складних експертних оцінок.

3. Синергія адміністративної превенції та кримінально-правової відповідальності в контексті повоєнного відновлення

Запропонований адміністративний механізм не замінює кримінальне реагування, а створює з ним двосторонній синергетичний зв'язок. Ця синергія є критично важливою для безпеки проєктів повоєнного відновлення, що будуть пов'язані з глибокою цифровізацією. Міжнародні інвестори дедалі частіше оцінюють рівень цифрової безпеки як ключовий фактор для прийняття рішень. Таким чином, превентивний механізм стає не лише інструментом захисту, а й стратегічною перевагою, що демонструє відповідність України стандартам безпечного розвитку, задекларованим в «Пакті в ім'я майбутнього» ООН[10].

Цей комплексний позитивний вплив проявляється у кількох напрямах. Насамперед, адміністративна превенція слугує доказовою базою для кримінальної юстиції. Наявність публічного реєстру створює правову презумпцію обізнаності. Службова особа, яка санкціонувала закупівлю забороненого ПЗ на ОКІ, не зможе посилатися на незнання. Це кардинально полегшує доказування суб'єктивної сторони (у формі злочинної недбалості) у складі злочину, передбаченого ст. 367 КК України.

Крім того, для посилення превентивного ефекту, свідоме порушення адміністративних заборон може бути криміналізовано. Наприклад, ч. 2 ст. 361 КК України можна доповнити кваліфікуючою ознакою:

[10] Pact for the Future : resolution adopted by the General Assembly on 22 September 2024. A/RES/79/1. URL: https://documents.un.org/doc/undoc/gen/N24/164/33/pdf/N2416433.pdf (дата звернення: 29.10.2025).

«...вчинені повторно... або з використанням програмного засобу, щодо якого уповноваженим органом встановлено заборону на використання на об'єктах критичної інфраструктури...».

Існує і зворотний зв'язок: матеріали кримінальних проваджень можуть слугувати офіційною підставою для внесення ПЗ до реєстру. Якщо розслідування показують, що певний легальний продукт систематично використовується для злочинів, це стане вагомим аргументом для комісії. Нарешті, у довгостроковій перспективі прозора система контролю стане важливим фактором інвестиційної привабливості, демонструючи здатність держави захищати цифрову інфраструктуру.

Більше того, наявність такого прозорого механізму відповідає сучасним глобальним інвестиційним трендам, зокрема, стандартам ESG (Environmental, Social, and Governance)[11]. Надійне управління ризиками у сфері кібербезпеки та захист критичної інфраструктури є невід'ємною складовою компонента «G» (Governance). Міжнародні інвестори та фінансові інституції, ухвалюючи рішення про фінансування проєктів повоєнного відновлення, дедалі частіше враховують не лише фінансові показники, а й стійкість та якість державного управління. Таким чином, запропонований механізм підвищує не тільки безпеку, але й інвестиційну репутацію держави.

Такий двосторонній обмін інформацією дозволяє створити замкнений цикл управління ризиками (risk management loop). Адміністративний орган, спираючись на дані правоохоронців, ідентифікує нові загрози та вносить ПЗ до реєстру (превенція). Це, у свою чергу, створює нові юридичні факти (презумпцію обізнаності, кваліфікуючі ознаки), які спрощують роботу слідчих та прокурорів у майбутніх провадженнях (реакція). Таким чином, система набуває здатності до самовдосконалення та адаптації до нових викликів

ВИСНОВКИ

Динаміка сучасних кіберзагроз вимагає від України переходу від фрагментарної реактивної протидії до комплексної проактивної стратегії. Кримінально-правові інструменти мають стати її завершальною, а не єдиною ланкою.

Формування цілісного адміністративно-правового механізму ідентифікації та обмеження обігу небезпечного ПЗ є нагальним завданням, що посилить превентивний захист та створить доказову базу для

[11] Що таке ESG-принципи і чому компаніям важливо їх дотримуватися. Fintech Insider. 16.11.2023. URL: https://fintechinsider.com.ua/shho-take-esg-prynczypy-i-chomu-kompaniyam-vazhlyvo-yih-dotrymuvatysya/ (дата звернення: 20.10.2025).

кримінальної юстиції. Розбудова такої системи є складовою зміцнення цифрового суверенітету та запорукою успішного повоєнного відновлення. Більше того, такий крок позиціонуватиме Україну як одного з лідерів у формуванні нової архітектури глобальної цифрової безпеки, втілюючи на національному рівні принципи, закладені в «Глобальному цифровому договорі» ООН.

Насамкінець, розробка та імплементація такого механізму є не лише актом національного самозахисту, а й внеском у формування міжнародної практики. Досвід України може стати моделлю стійкості (resilience model) для інших країн, демонструючи, як принципи адміністративного права можуть бути ефективно застосовані для нейтралізації сучасних гібридних загроз.

Зрештою, імплементація такого національного механізму може стати першим кроком до формування нової архітектури міжнародної цифрової безпеки. У майбутньому можливе укладення двосторонніх або багатосторонніх угод про взаємне визнання національних реєстрів небезпечного ПЗ між країнами-партнерами. Це дозволить створити своєрідну «коаліцію цифрової довіри» – групу держав, які спільно протидіють розповсюдженню програмних продуктів від авторитарних режимів, тим самим посилюючи колективну стійкість демократичного світу до гібридних загроз.

Впровадження запропонованої моделі також потребуватиме розвитку відповідної експертної та судової практики. Судді адміністративних судів, розглядаючи скарги на рішення міжвідомчої комісії, стикатимуться з необхідністю оцінювати складні технічні та геополітичні аргументи. Це вимагатиме підвищення кваліфікації судового корпусу та, можливо, залучення судових експертів у галузі кібербезпеки. Формування сталої судової практики у цій категорії справ стане фінальним етапом інституціоналізації механізму та його інтеграції в національну правову систему.

АНОТАЦІЯ

У розділі здійснено доктринальний аналіз неефективності існуючої реактивної кримінально-правової моделі протидії програмним загрозам національній безпеці, особливо в контексті гібридної війни. На основі аналізу глобальних тенденцій, зокрема ініціативи ООН щодо «Глобального цифрового договору», обґрунтовується необхідність парадигмального зсуву до проактивної системи адміністративно-правової превенції. Доведено, що класичні інструменти кримінальної юстиції стикаються з практично нездоланними викликами атрибуції атак (особливо APTs), доказування умислу розробників ПЗ подвійного

призначення та визначення юрисдикції. Розкрито зміст доктринальної категорії «програмне забезпечення, що становить загрозу національній безпеці» та запропоновано концептуальну модель превентивного адміністративно-правового механізму. Ця модель включає створення міжвідомчого уповноваженого органу, розробку публічної методики оцінки ризиків, ведення реєстру небезпечного ПЗ та застосування диференційованих правових режимів, що ґрунтуються на принципі пропорційності. Окремо досліджено синергетичний зв'язок між адміністративною превенцією та кримінальною відповідальністю, де запропонований механізм створює доказову базу для кримінальної юстиції (презумпцію обізнаності) та водночас використовує її дані для ідентифікації загроз, формуючи замкнений цикл управління ризиками. Обґрунтовано, що такий механізм не лише посилить превентивний потенціал держави, а й позитивно вплине на інвестиційний клімат у процесі повоєнного відновлення.

Література

1. Pact for the Future : resolution adopted by the General Assembly on 22 September 2024. A/RES/79/1. URL: https://documents.un.org/doc/undoc/gen/N24/164/33/pdf/N2416433.pdf.
2. Звіт про результати роботи у 2024 році / Національна поліція України. Київ, 2025. 18 с. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2024/zvit-npu-2024.pdf.
3. Internet Crime Report 2024 / Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). 2025. 47 p. URL: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
4. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. Відомості Верховної Ради України. 2001. № 25–26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14.
5. Cybersecurity Handbook: Best Practices for the Protection and Resilience of Network and Information Systems / Hellenic Republic, Ministry of Digital Governance, National Cybersecurity Authority. June 2021. 76 p. URL: https://cyber.gov.gr/wp-content/uploads/2025/03/Cybersecurity-Handbook-English-version-compressed.pdf.
6. Internet Organised Crime Threat Assessment (IOCTA) 2024 / Europol. 2024. 76 p. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf.
7. Where can I find the Entity List? / U.S. Department of Commerce, Bureau of Industry and Security. URL: https://www.bis.doc.gov/index.php/component/fsj_faqs/faq/106-where-can-i-find-the-entity-lis.

8. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union. 27.12.2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02022L2555-20221227.

9. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» : Указ Президента України від 26.08.2021 р. № 447/2021. *Офіційний вісник України.* 2021. № 68. Ст. 4295. URL: https://zakon.rada.gov.ua/laws/show/447/2021.

10. Що таке ESG-принципи і чому компаніям важливо їх дотримуватися. Fintech Insider. 16.11.2023. URL: https://fintechinsider.com.ua/shho-take-esg-prynczypy-i-chomu-kompaniyam-vazhlyvo-yih-dotrymuvatysya/.

Information about the authors:
Yevdokymenko Denys Mykolayovich,
PhD student at the
Kyiv University of Law of the National Academy
of Sciences of Ukraine,
Expert of the IT & Telecom sector at the Better Regulation Delivery
Office (BRDO), Kyiv
7A Akademika Dobrokhotova Str., Kyiv, 03142, Ukraine

Malii Mykola Ivanovych,
PhD in Law,
Associate Professor at the Department of Criminal Law and Procedure
Kyiv University of Law of the National Academy
of Sciences of Ukraine,
7A, Akademika Dobrokhotova Str., Kyiv, 03142, Ukraine