УДК 004.94

https://doi.org/10.52058/3041-1254-2025-12(22)-1440-1450

Ткаченко Олександр Іванович викладач кафедри інформаційної безпеки ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», https://orcid.org/0009-0001-9073-5814

ЕФЕКТИВНІСТЬ ПУБЛІЧНО-УПРАВЛІНСЬКИХ ІНСТРУМЕНТІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЙ ТА ПІДПРИЄМСТВ УКРАЇНИ

Анотація. Стаття присвячена дослідженню ефективності публічно-управлінських інструментів забезпечення інформаційної безпеки організацій та підприємств України в умовах цифровізації управлінських процесів і зростання кіберризиків, зумовлених гібридними загрозами та воєнним контекстом. У фокусі уваги перебувають управлінські рішення, що реалізуються через нормативно-правове регулювання, інституційний нагляд, координацію між суб'єктами сектору безпеки і бізнесом, а також механізми превенції, реагування та відновлення.

Проаналізовано практичні аспекти застосування державних політик і процедур управління інформаційною безпекою на рівні організацій та підприємств, зокрема підходи до ризик-орієнтованого менеджменту, аудиту та моніторингу, стандартизації вимог до захисту даних і критичних інформаційних ресурсів, а також роль цифрових сервісів держави у підтримці безпечного обігу інформації. Виявлено ключові проблеми: фрагментарність регулювання, нерівномірність спроможностей суб'єктів господарювання, дефіцит кадрів та недостатня інтегрованість інформаційно-аналітичних контурів.

Аргументовано, що результативність публічно-управлінських інструментів визначається не лише формальним запровадженням норм і контролю, а й якістю міжвідомчої взаємодії, наявністю зрозумілих KPI, спроможністю забезпечити доказову базу інцидентів, швидкі канали повідомлення та правову визначеність відповідальності сторін. Обґрунтовано доцільність поєднання регуляторного підходу з сервісно-орієнтованими механізмами підтримки бізнесу, включно з методичними рекомендаціями, типовими політиками безпеки, навчанням персоналу та стимулюванням впровадження стандартів.

Окремої уваги заслуговує питання оцінювання ефективності: запропоновано розглядати її як багатовимірну категорію, що охоплює інституційну спроможність, рівень відповідності вимогам, інцидентну стійкість і здатність до відновлення, а також соціальний ефект у вигляді захисту прав працівників і клієнтів та збереження довіри до цифрових сервісів. Наголошено на пріоритет-

ності побудови єдиних підходів до звітності про інциденти, розвитку культури кібергігієни та підвищення узгодженості державних програм із потребами реального сектору.

Ключові слова: публічне управління, інформаційна безпека, організації та підприємства, кіберризики, управління ризиками, державне регулювання, інституційна спроможність, цифровізація, KPI, стійкість.

Tkachenko Oleksandr Ivanovych lecturer at the Department of Information Security, PJSC “Higher Educational Institution ”Interregional Academy of Personnel Management", https://orcid.org/0009-0001-9073-5814

EFFECTIVENESS OF PUBLIC ADMINISTRATION TOOLS FOR ENSURING INFORMATION SECURITY OF ORGANIZATIONS AND ENTERPRISES IN UKRAINE

Abstract. The article is devoted to the study of the effectiveness of public-administration instruments for ensuring information security in organizations and enterprises of Ukraine under conditions of managerial digitalization and increasing cyber risks driven by hybrid threats and the wartime context. The focus is placed on governance decisions implemented through regulatory frameworks, institutional oversight, coordination between the security sector and business, as well as mechanisms of prevention, response, and recovery.

It is analyzed the practical aspects of applying state policies and procedures of information security management at the level of organizations and enterprises, in particular risk-oriented management approaches, audit and monitoring, standardization of requirements for data protection and critical information resources, and the role of government digital services in supporting secure information circulation. Key problems are identified: fragmented regulation, uneven capacities of economic actors, staff shortages, and insufficient integration of information-analytical contours.

It is argued that the effectiveness of public-administration instruments is determined not only by the formal introduction of rules and control, but also by the quality of interagency cooperation, the availability of clear KPIs, the ability to build an evidence base for incidents, fast reporting channels, and legal certainty regarding the responsibilities of the parties. The expediency of combining a regulatory approach with service-oriented mechanisms to support business is substantiated, including methodological guidance, model security policies, personnel training, and incentives for implementing standards.

Particular attention is paid to the issue of effectiveness assessment: it is proposed to treat it as a multidimensional category that covers institutional capacity, the level of compliance with requirements, incident resilience and recovery capability, as well as the social effect in the form of protecting the rights of employees and clients and

maintaining trust in digital services. The priority is emphasized of establishing unified approaches to incident reporting, developing a culture of cyber hygiene, and increasing the alignment of state programs with the needs of the real sector.

Keywords: public administration, information security, organizations and enterprises, cyber risks, risk management, state regulation, institutional capacity, digitalization, KPIs, resilience.

Постановка проблеми. Стрімка цифровізація управлінських і виробничих процесів в Україні, масове використання хмарних сервісів, електронного документообігу та віддалених форматів роботи підвищили залежність організацій і підприємств від стійкості інформаційних систем та якості захисту даних. Водночас воєнні дії й гібридна агресія актуалізували системні кібератаки, дезінформаційні кампанії та цілеспрямовані порушення доступності критичних сервісів, що безпосередньо впливають на безперервність діяльності, фінансову стабільність, охорону комерційної таємниці та захист прав працівників і клієнтів.

Незважаючи на наявність нормативно-правових засад і діяльність профільних інституцій, практична реалізація публічно-управлінських інструментів забезпечення інформаційної безпеки характеризується нерівномірністю спроможностей суб'єктів господарювання, фрагментарністю процедур координації, недостатньою стандартизацією вимог до управління ризиками та інцидентами, а також дефіцитом ресурсів і компетентностей. Це зумовлює розрив між формальними регуляторними приписами та фактичною стійкістю організацій до кіберінцидентів, що ускладнює формування належної доказової бази, своєчасне реагування, досудовий розгляд справ і забезпечення ефективного судового захисту у разі порушень.

У таких умовах постає науково-прикладна проблема оцінювання ефективності публічно-управлінських інструментів у сфері інформаційної безпеки та визначення напрямів їх удосконалення на основі ризик-орієнтованого підходу, прозорих критеріїв результативності й узгоджених механізмів взаємодії держави та бізнесу. Відсутність уніфікованих показників ефективності й інституційно закріплених процедур моніторингу знижує керованість сфери, послаблює довіру до цифрових сервісів і збільшує соціально-економічні втрати, що й зумовлює актуальність дослідження.

Аналіз останніх досліджень і публікацій. У сучасному науковому дискурсі проблематика забезпечення інформаційної безпеки організацій та підприємств розглядається як міждисциплінарний напрям, що поєднує публічне управління, інформаційне право, кібербезпеку, менеджмент ризиків і комплаєнс. Дослідження останніх років переважно фокусуються на еволюції державної політики у сфері кібербезпеки, інституційній архітектурі координації, впровадженні ризик-орієнтованих моделей управління та розвитку національних механізмів реагування на інциденти. Окремий пласт публікацій присвячений узгодженню

національних підходів із європейськими рамками цифрової стійкості, вимогами до захисту критично важливих послуг і практиками безпеки ланцюгів постачання.

У працях, присвячених цифровим комунікаціям, кібербезпеці та управлінським механізмам у публічному секторі й суміжних сферах, питання забезпечення інформаційної безпеки та кіберстійкості розглядали, зокрема, Віннічук І., Герасимюк К., Жекало Г. І., Заяць М., Забейворота Т., Коваленко О., Ковбасюк Ю., Колодій А., Ліпінська А. Отже, попри наявність значного масиву публікацій, актуальною є потреба в систематизації підходів саме до вимірювання ефективності публічно-управлінських інструментів забезпечення інформаційної безпеки в організаціях та підприємствах України, із врахуванням інституційної взаємодії, процедурних аспектів доказування, практик комплаєнсу й цифрової стійкості. Це формує підґрунтя для подальшого дослідження, спрямованого на уточнення критеріїв оцінювання та визначення напрямів удосконалення управлінських механізмів у зазначеній сфері.

Метою дослідження є оцінювання ефективності публічно-управлінських інструментів забезпечення інформаційної безпеки організацій та підприємств України й обґрунтування напрямів їх удосконалення на основі ризик-орієнтованого підходу, узгоджених критеріїв результативності та міжвідомчої координації.

Виклад основного матеріалу. У сучасних умовах війни та прискореної цифровізації інформаційна безпека організацій і підприємств України перетворилася на елемент публічного інтересу, оскільки збої в ІКС бізнесу, фінансових установ і постачальників послуг швидко набувають суспільного виміру через порушення ланцюгів постачання, блокування платежів, зупинку сервісів підтримки населення та зростання вторинних ризиків для державних реєстрів, критичної інфраструктури й систем соціального захисту. У такій конфігурації ефективність публічно-управлінських інструментів має оцінюватися не декларативно, а через здатність державної політики формувати зрозумілі правила, забезпечувати нагляд і стимулювати інвестиції в кіберстійкість, водночас мінімізуючи адміністративні бар'єри для доброчесного бізнесу, адже надмірне регулювання без інструментів підтримки переорієнтовує ресурси підприємств на формальну звітність, а не на реальне зниження ризику. Правова рамка визначає базові принципи та суб'єктність у сфері кібербезпеки, закріплюючи роль координаційних механізмів і повноваження державних органів, а також вводячи нормативне поле для взаємодії держави й приватного сектору, у межах якого підприємства мають будувати систему управління ризиками та захисту критичних процесів; у цьому контексті законодавчі засади, закріплені профільним законом про кібербезпеку [1], доцільно трактувати як фундамент не лише для державних ІКС, а й для корпоративного управління безпекою на рівні підприємств, які обслуговують масові послуги, фінанси, логістику й енергозабезпечення.

Управлінська результативність правових норм проявляється через їх операціоналізацію в політиках, процедурах і контрольних практиках, а також через захист прав людини у цифровому середовищі, бо витік або компрометація даних перетворює кібератаку на правопорушення з матеріальними збитками, репутаційними втратами й потенційними соціальними наслідками, що особливо відчутно в секторах із великими масивами персональної інформації. Вимоги щодо належної обробки персональних даних, обмеження доступу, визначення ролей володільця та розпорядника, а також принципи законності й пропорційності в обробці формують мінімальний стандарт організаційної дисципліни, який, будучи підкріпленим державним наглядом і внутрішнім контролем, знижує імовірність інцидентів, пов'язаних із несанкціонованим доступом, помилками персоналу та некоректною конфігурацією прав; саме тому інтеграція вимог законодавства про персональні дані у внутрішні програми кіберзахисту [2] виступає індикатором зрілості публічно-управлінського підходу, коли регуляторні приписи не існують окремо від ризик-менеджменту, а стають його части-ною через політики доступу, журналювання, сегментацію і навчання персоналу.

Окремий рівень вимог виникає там, де підприємства належать до критично важливих або обслуговують критичні функції, оскільки зупинка їх діяльності створює каскадний ефект для територіальних громад, економіки та держави, що зумовлює необхідність спеціальних механізмів ідентифікації об'єктів, категоризації ризиків та планування безперервності. У площині публічного управління ефективність у цій сфері визначається тим, наскільки держава здатна узгодити вимоги безпеки з реальними спроможностями операторів, забезпечити методичну підтримку, а також створити умови для взаємодії між регуляторами, правоохоронними структурами та власниками інфраструктури; у цьому сенсі положення закону про критичну інфраструктуру [3] доцільно розглядати як рамку, що легітимує ризик-орієнтовані підходи, коли пріоритетом стає не формальна відповідність, а захист життєво важливих сервісів, резервування, відновлення та готовність до інцидентів із вимірюваними параметрами часу простою й допустимих втрат.

Емпірично потреба в таких інструментах підтверджується масштабом цифрової економіки та залежністю населення від електронних транзакцій, де навіть короткочасне порушення доступності провокує соціальне напруження і ризики для довіри до фінансових інститутів. За даними Національного банку України, у 2024 році кількість операцій з використанням платіжних карток, емітованих українськими банками та фінансовими установами, становила 8 654,4 млн, а загальна сума таких операцій дорівнювала 6 577,4 млрд грн, при цьому в Україні здійснено 91,8 відсотка від кількості та 90,1 відсотка від суми всіх операцій [4], що демонструє високу концентрацію фінансових потоків у цифрових каналах і пояснює, чому кібератаки на платіжну інфраструктуру,

процесинг, банківські ІКС та постачальників цифрових сервісів стають не лише корпоративною проблемою, а й питанням публічної політики.

Соціальний вимір кіберстійкості ще виразніше простежується через залежність бюджетних видатків і соціальних програм від надійності інформаційних систем держави, банків і платіжних посередників, оскільки затримка або компрометація процесів виплат у кризових умовах одразу створює ризики для вразливих груп та підриває легітимність інститутів. У 2024 році, за офіційною інформацією, з державного бюджету в повному обсязі профінансовано соціальні виплати на 447,9 млрд грн, зокрема 274,7 млрд грн спрямовано на фінансове забезпечення виплати пенсій, надбавок та підвищень до пенсій і покриття дефіциту відповідних пенсійних програм [5], тому ефективність публічно-управлінських інструментів у сфері інформаційної безпеки має оцінюватися також через показники безперервності критичних соціальних процесів, стійкості платіжних і реєстрових систем, а також здатності держави й фінансового сектору забезпечити захищену ідентифікацію отримувачів, цілісність даних і надійність каналів доставки коштів.

Оцінювання ефективності інструментів регулювання неможливе без урахування реального ландшафту інцидентів, оскільки саме він відображає, чи спрацьовують профілактичні та реактивні механізми, чи домінує модель постфактумного реагування. Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA у 2024 році опрацювала 4 315 кіберінцидентів [6], а в повідомленнях також акцентовано на зростанні навантаження та типовості векторів, що в сукупності вказує на потребу зміщення управлінського фокусу з фрагментарних заходів на системні програми кібергігієни, сегментації мереж, контролю привілейованих доступів, резервного копіювання й тестування відновлення, а також на інституційне закріплення обміну інформацією про загрози між державою і приватним сектором у форматах, придатних для швидкого впровадження на підприємствах різного масштабу.

Практика нагляду у фінансовому секторі демонструє, як публічно-управлінські інструменти можуть бути перетворені на конкретні організаційні вимоги з прозорими критеріями контролю, при цьому важливо, щоб такі вимоги містили не лише загальні декларації, а й вимірювані параметри процесів, відповідальності та незалежної перевірки. Положення про організацію кіберзахисту в банківській системі України, затверджене постановою НБУ № 178 [7], важливе тим, що переводить кіберзахист у площину управління ризиками й корпоративного управління, де ключовими стають роль керівництва, визначення критичних функцій, управління інцидентами, регулярні аудити та контроль постачальників, а також дисципліна змін і конфігурацій, що для підприємств поза банківською сферою може виступати практичним шаблоном для адаптації внутрішніх політик і процедур безпекового менеджменту.

Ефективність інструментів посилюється тоді, коли регуляторні вимоги оновлюються з урахуванням розвитку загроз і технологій, а також коли вони

пов'язані з механізмами відповідальності та внутрішнього контролю, а не зводяться до формального виконання мінімуму. Показовим є оновлення вимог до управління доступом, автентифікації, протоколювання та контролю використання змінних носіїв у нормативних документах НБУ, оприлюднених у грудні 2025 року, де акцент зроблено на внутрішніх документах надавача фінансових послуг і включенні інформаційної безпеки до системи управління ризиками [8]; у ширшому публічно-управлінському вимірі такий підхід варто розглядати як орієнтир для секторальних регуляторів і органів місцевого самоврядування, які закуповують цифрові послуги або експлуатують інформаційні системи, адже він демонструє інструментальний характер норм, орієнтованих на процеси та контрольні точки, а не на формальне декларування відповідності.

Глобальні тенденції підтверджують, що ключові втрати для організацій і підприємств спричиняють не лише витоки даних, а й атаки на доступність, компрометація облікових даних, вразливості на межі мережі та рекетирські моделі вимагання, які перетворюють інцидент на кризу управління, що потребує синхронізації юридичних, комунікаційних, IT та фінансових рішень. За матеріалами Verizon Data Breach Investigations Report 2025, у структурі сучасних інцидентів виразно простежується зростання системних вторгнень і вагомість ransomware-компоненти, а також значущість ланцюгів постачання та третіх сторін, що підтверджує доцільність державної політики, спрямованої на мінімальні стандарти безпеки постачальників і контрактні вимоги до кіберзахисту для закупівель [9]; у практичній площині для українських підприємств це означає необхідність переходу від точкових технічних засобів до зрілої моделі управління ризиком, де ключовими індикаторами стають середній час виявлення та локалізації, готовність резервних копій, контроль привілейованих доступів, а також реальна здатність відновлювати критичні сервіси у визначений час без втрати цілісності даних.

Український досвід наочно демонструє, що кіберінциденти здатні створювати макроефект, навіть коли формально спрямовані проти одного суб'єкта господарювання, оскільки у цифрових екосистемах домінують мережеві залежності, а населення сприймає доступність зв'язку, платежів і сервісів як базову умову безпеки повсякдення. Після масштабної кібератаки на найбільшого мобільного оператора материнська компанія оцінювала збитки приблизно у 3,6 млрд грн [10], що підкреслює, що ефективність публічно-управлінських інструментів не може вимірюватися лише кількістю нормативних актів або наявністю профільних підрозділів, а має оцінюватися через здатність держави разом із приватним сектором забезпечувати резервування, взаємодію з національними командами реагування, координацію з правоохоронними органами, кризові комунікації, а також відновлення критичних функцій із мінімізацією соціально-економічних втрат.

Узагальнюючи, ефективність публічно-управлінських інструментів забезпечення інформаційної безпеки організацій та підприємств України доцільно розкривати як комплексну характеристику, що поєднує нормативно-правову визначеність, інституційну спроможність, наглядові та стимулюючі механізми, якісну координацію реагування, а також практичну здатність секторів економіки підтримувати безперервність критичних процесів, зокрема платежів і соціально значущих сервісів. Результативність підвищується тоді, коли правила стають зрозумілими й вимірюваними, контроль переходить від формальної перевірки документів до оцінювання процесів і фактичної готовності, а стимули орієнтовані на інвестиції в стійкість, включно з резервним живленням, дублюванням каналів зв'язку, безпечною хмарною інфраструктурою, навчанням персоналу та перевіркою постачальників. Водночас на рівні підприємств ключовою умовою виступає перетворення інформаційної безпеки на компонент корпоративного управління, де ризики вимірюються фінансово та операційно, відповідальність закріплюється за керівництвом, а контроль вбудовується у бізнес-процеси, що дає змогу поєднати вимоги державної політики з економічною доцільністю та суспільною відповідальністю.

Висновки. Проведений аналіз дає підстави стверджувати, що ефективність публічно-управлінських інструментів забезпечення інформаційної безпеки організацій та підприємств України визначається не кількістю прийнятих нормативних актів, а їх здатністю трансформуватися у дієві управлінські практики на рівні конкретних суб'єктів господарювання. За умов війни та гібридних загроз інформаційна безпека набуває ознак публічного блага, оскільки інциденти в приватному секторі швидко переходять у площину суспільних ризиків, впливають на стабільність сервісів, безперервність соціально значущих процесів і довіру до цифрових каналів взаємодії з державою та фінансовою системою.

Емпіричні дані підкреслюють масштаб залежності економіки й населення від цифрових інфраструктур: у 2024 році зафіксовано 8 654,4 млн операцій з платіжними картками на суму 6 577,4 млрд грн, а обсяг профінансованих соціальних виплат у 2024 році становив 447,9 млрд грн, що демонструє критичність стійкості платіжних, реєстрових та суміжних інформаційних систем. Паралельно реальний ландшафт загроз підтверджується практикою реагування, зокрема опрацюванням 4 315 кіберінцидентів CERT-UA у 2024 році, а також значними економічними втратами від окремих масштабних атак, які можуть оцінюватися у мільярдах гривень. Отже, предмет оцінювання ефективності має виходити за межі формальної відповідності та фокусуватися на вимірюваних показниках кіберстійкості, здатності до реагування та відновлення.

Окремого значення набуває питання інституційної координації та доказовості, адже кіберінцидент часто перетворюється на юридичний спір щодо

відповідальності сторін, належності заходів захисту та розміру завданих збитків. Тому підвищення ефективності публічно-управлінських інструментів пов'язане з упорядкуванням процедур фіксації та документування інцидентів, стандартизацією підходів до звітності, розвитком каналів оперативного обміну інформацією про загрози між державою та бізнесом, а також з інтеграцією безпекових вимог у публічні закупівлі й контракти з постачальниками цифрових послуг. Саме поєднання регуляторного впливу з сервісно-орієнтованою підтримкою, навчанням і стимулюванням впровадження стандартів створює умови, за яких дотримання вимог стає економічно й організаційно раціональним.

У підсумку, забезпечення інформаційної безпеки в організаціях та на підприємствах України потребує переходу до моделі управління, де пріоритетом є стійкість критичних процесів, вимірюваність результатів та відповідальність за ризики на рівні керівництва, а публічне управління виконує не лише контрольну, а й координаційну та підтримувальну функцію. Перспективним напрямом є формування єдиних критеріїв оцінювання ефективності з прив'язкою до показників безперервності, часу виявлення й локалізації інцидентів, здатності до відновлення, якості управління доступами та готовності до кризових сценаріїв, що дозволить підвищити практичну керованість сфери і зменшити як економічні, так і соціальні наслідки кіберзагроз.

Література:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних Законодавство України / Верховна Рада України. URL: https:// zakon.rada.gov.ua/go/2163-19 (дата звернення: 14.12.2025).

2. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // База даних Законодавство України / Верховна Рада України. URL: https:// zakon.rada.gov.ua/go/2297-17 (дата звернення: 14.12.2025).

3. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX // База даних Законодавство України / Верховна Рада України. URL: https:// zakon.rada.gov.ua/go/1882-20 (дата звернення: 14.12.2025).

4. Безготівкові розрахунки у 2024 році суттєво переважали серед операцій з платіжними картками. 03.03.2025 // Офіційний сайт НБУ. URL: https:// bank.gov.ua/ua/news/all/bezgotivkovi-rozrahunki-u-2024-rotsi-suttyevo-perevajali-sered-operatsiy-z-platijnimi-kartkami (дата звернення: 14.12.2025).

5. Мінфін: У 2024 році в повному обсязі профінансовано соцвиплати на 447,9 млрд грн. 09.01.2025 // Урядовий портал. URL: https:// www.kmu.gov.ua/news/minfin-u-2024-rotsi-v-povnomu-obsiazi-profinansovano-sotsvyplaty-na-4479-mlrd-hrn (дата звернення: 14.12.2025).

6. Державна служба спеціального зв'язку та захисту інформації України. CERT-UA минулого року опрацювала 4315 кіберінцидентів. 08.01.2025 // Офіційний сайт. URL: https:// cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення: 14.12.2025).

7. Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України : Постанова Національного банку України від 12.08.2022 № 178 // База даних Законодавство України / Верховна Рада України. URL: https:// zakon.rada.gov.ua/go/v0178500-22 (дата звернення: 14.12.2025).

8. Постанова Правління НБУ (нормативний акт щодо організації заходів з інформаційної безпеки та внутрішніх вимог до безпеки інформації). 09.12.2025 // Офіційний сайт НБУ (PDF). URL: https:// bank.gov.ua/admin_uploads/law/09122025_143.pdf (дата звернення: 14.12.2025).

9. 2025 Data Breach Investigations Report. 2025 // Verizon Business (PDF). URL: https:// www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf (дата звернення: 14.12.2025).

10. Материнська компанія Київстару назвала суму збитків внаслідок кібератаки. 18.01.2024 // Суспільне Новини. URL: https:// suspilne.media/664234-materinska-kompania-kiivstaru-nazvala-sumu-zbitkiv-vnaslidok-kiberataki/ (дата звернення: 14.12.2025).

References:

1. National Bank of Ukraine. (2022, August 12). Postanova Pravlinnia Natsionalnoho banku Ukrainy № 178: Polozhennia pro orhanizatsiiu kiberzakhystu v bankivskii systemi Ukrainy ta vnesennia zmin do Polozhennia pro vyznachennia obiektiv krytychnoi infrastruktury v bankivskii systemi Ukrainy [Resolution of the Board of the National Bank of Ukraine No. 178: Regulation on organizing cyber protection in the banking system of Ukraine and amendments regarding identification of critical infrastructure objects in the banking system of Ukraine]. Zakonodavstvo Ukrainy. Retrieved from https:// zakon.rada.gov.ua/go/v0178500-22 [in Ukrainian].

2. National Bank of Ukraine. (2025, March 3). Bezghotivkovi rozrakhunky u 2024 rotsi suttievo perevazhaly sered operatsii z platizhnymy kartkamy [Cashless payments in 2024 significantly prevailed among payment card transactions]. National Bank of Ukraine. Retrieved from https:// bank.gov.ua/ua/news/all/bezgotivkovi-rozrahunki-u-2024-rotsi-suttyevo-perevajali-sered-operatsiy-z-platijnimi-kartkami [in Ukrainian].

3. National Bank of Ukraine. (2025, December 9). Postanova Pravlinnia Natsionalnoho banku Ukrainy shchodo orhanizatsii zakhodiv z informatsiinoi bezpeky ta vnutrishnikh vymoh do bezpeky informatsii [Resolution of the Board of the National Bank of Ukraine on organizing information security measures and internal information security requirements]. National Bank of Ukraine. Retrieved from https:// bank.gov.ua/admin_uploads/law/09122025_143.pdf [in Ukrainian].

4. Ministry of Finance of Ukraine. (2025, January 9). Minfin: U 2024 rotsi v povnomu obsiazi profinasovano sotsvyplaty na 447,9 mlrd hrn [In 2024, social payments were fully financed in the amount of UAH 447.9 billion]. Government Portal of Ukraine. Retrieved from https:// www.kmu.gov.ua/news/minfin-u-2024-rotsi-v-povnomu-obsiazi-profinansovano-sotsvyplaty-na-4479-mlrd-hrn [in Ukrainian].

5. State Service of Special Communications and Information Protection of Ukraine. (2025, January 8). CERT-UA mynuloho roku opratsiuvala 4315 kiberintsydentiv [CERT-UA processed 4,315 cyber incidents last year]. State Service of Special Communications and Information Protection of Ukraine. Retrieved from https:// cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv [in Ukrainian].

6. Suspilne Novyny. (2024, January 18). Materynska kompaniia Kyivstaru nazvala sumu zbytkiv vnaslidok kiberataky [Kyivstar's parent company named the amount of losses due to the cyberattack]. Suspilne. Retrieved from https:// suspilne.media/664234-materinska-kompania-kiivstaru-nazvala-sumu-zbitkiv-vnaslidok-kiberataki/ [in Ukrainian].

7. Verizon. (2025). 2025 Data Breach Investigations Report. Verizon Business. Retrieved from https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf [in English].

8. Verkhovna Rada of Ukraine. (2010, June 1). Zakon Ukrainy Pro zakhyst personalnykh danykh № 2297-VI [Law of Ukraine on personal data protection No. 2297-VI]. Zakonodavstvo Ukrainy. Retrieved from https:// zakon.rada.gov.ua/go/2297-17 [in Ukrainian].

9. Verkhovna Rada of Ukraine. (2017, October 5). Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy № 2163-VIII [Law of Ukraine on basic principles of cybersecurity of Ukraine No. 2163-VIII]. Zakonodavstvo Ukrainy. Retrieved from https:// zakon.rada.gov.ua/go/2163-19 [in Ukrainian].

10. Verkhovna Rada of Ukraine. (2021, November 16). Zakon Ukrainy Pro krytychnu infrastrukturu № 1882-IX [Law of Ukraine on critical infrastructure No. 1882-IX]. Zakonodavstvo Ukrainy. Retrieved from https:// zakon.rada.gov.ua/go/1882-20 [in Ukrainian].