https://doi.org/10.31891/2307-5740-2026-350-48
УДК 004.056.5:336.71
JEL classification: G21, G28, D83, O33, L86

ЗАЯЧКІВСЬКА Оксана
Національний університет водного господарства та природокористування
https://orcid.org/0000-0002-8792-9204
e-mail: o.v.zaychkivska@gmail.com
ШВЕЦЬ Віктор
Національний університет водного господарства та природокористування
https://orcid.org/0009-0008-3751-9101
e-mail: shvets.v_em24@nuwm.edu.ua
ІЛЛІН Вадим
Національний університет водного господарства та природокористування
https://orcid.org/0009-0002-9695-5655
e-mail: v.v.illin@nuwm.edu.ua

СУТНІСТЬ ТА ЗНАЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

У статті розглянуто сутність та значення інформаційної безпеки в банківській діяльності в умовах цифровізації та зростання кіберзагроз. Проаналізовано наукові й нормативні підходи до визначення інформаційної безпеки та її ключових характеристик: конфіденційності, цілісності й доступності. Визначено основні загрози інформаційній безпеці банківських установ і обґрунтовано необхідність комплексного підходу до захисту інформаційних ресурсів як чинника фінансової стабільності та довіри клієнтів.

Ключові слова: інформаційна безпека, банківська діяльність, кіберзагрози, захист інформації, цифровізація.

ZAIACHKIVSKA Oksana, SHVETS Viktor, ILLIN Vadym
National University of Water and Environmental Engineering

THE ESSENCE AND SIGNIFICANCE OF INFORMATION SECURITY IN BANKING ACTIVITIES

The article is devoted to an in-depth study of the essence, role, and practical significance of information security in banking activities under the conditions of intensive digital transformation of the financial sector and the rapid growth of cyber threats. The relevance of the research is substantiated by the expansion of digital and remote banking services, the increasing dependence of banks on information technologies, the escalation of cybercrime, and the additional risks caused by the hybrid war against Ukraine, which has significantly intensified threats to critical financial infrastructure.

The paper analyzes scientific approaches to defining information security and systematizes its interpretation as a complex economic, organizational, and technological category aimed at protecting information resources, information systems, and data flows of banking institutions. Special attention is paid to the regulatory and legal framework governing information security in Ukraine, including its alignment with international standards and best practices in the field of cybersecurity and risk management.

The key characteristics of information security—confidentiality, integrity, and availability—are identified and their decisive role in ensuring the continuity of banking operations, financial stability, and reliability of payment systems is emphasized. The study outlines the main threats to information security in the banking sector, such as phishing attacks, fraudulent financial transactions, distributed denial-of-service (DDoS) attacks, unauthorized access to information systems, malware, and social engineering methods targeting bank employees and customers.

The article generalizes modern approaches to building a comprehensive information security system in banking institutions, which combines legal, organizational, technical, personnel, and managerial measures. It is substantiated that information security should be integrated into the strategic management system of banks and considered not only as a technical function, but also as a key component of corporate governance and risk management. Ensuring a high level of information security is defined as a prerequisite for strengthening customer trust, maintaining competitiveness, and achieving sustainable development of banking institutions in the digital economy.

Keywords: information security, banking, cyber threats, information protection, digitalization.

Стаття надійшла до редакції / Received 17.12.2025
Прийнята до друку / Accepted 23.01.2026
Опубліковано / Published 29.01.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

На сучасному етапі розвитку фінансово-економічної системи України спостерігається інтенсивне впровадження цифрових технологій у банківську діяльність та розширення спектра електронних фінансових послуг. Банківські установи, зокрема АТ «Сенс Банк», активно використовують дистанційні канали обслуговування клієнтів, такі як інтернет-банкінг, мобільні застосунки та електронні платіжні системи. Це сприяє підвищенню зручності й доступності банківських послуг, проте водночас зумовлює зростання загроз у сфері захисту інформації.

Інформаційні ресурси банку мають стратегічне значення, оскільки включають конфіденційні фінансові відомості клієнтів і внутрішню службову інформацію установи. Несанкціонований доступ або втрата таких даних можуть призвести до значних фінансових збитків, втрати ділової репутації, зниження рівня довіри клієнтів та настання правових наслідків. У зв'язку з цим забезпечення належного рівня інформаційної безпеки набуває першочергового значення та є важливою складовою стратегічного розвитку банківських установ.

За інформацією Національного банку України, протягом 2023 – 2024 років спостерігається зростання кількості кіберінцидентів у банківському секторі. Найбільш поширеними загрозами залишаються фішингові кампанії, шахрайські операції з платіжними картками, несанкціоноване втручання в роботу інформаційних систем, DDoS-атаки, а також методи соціальної інженерії, спрямовані як на клієнтів банків, так і на їхніх працівників. За таких умов особливої ваги набуває необхідність формування та впровадження ефективних систем захисту інформації, що відповідатимуть міжнародним стандартам безпеки (ISO/IEC 27001, NIST, PCI DSS) і нормативним вимогам регулятора.

Актуальність даного дослідження обумовлена також тим, що в умовах гібридної війни проти України банківські установи зазнають підвищеного рівня кіберзагроз. Атаки на об'єкти критичної фінансової інфраструктури спрямовані не лише на завдання економічних втрат, але й на підрив стабільності державної системи загалом. У цьому контексті досвід та практичні підходи до забезпечення інформаційної безпеки в АТ «Сенс Банк» є показовими й доцільними для подальшого наукового аналізу.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

У сучасних умовах інформація набула статусу одного з ключових стратегічних ресурсів. Якщо раніше вирішальну роль в економічному розвитку відігравали природні ресурси, фінансовий капітал і трудовий потенціал, то нині саме інформація визначає ефективність функціонування та рівень конкурентоспроможності організацій у різних сферах діяльності.

В умовах збройної агресії проти України інформаційний простір фактично став окремим напрямом протистояння, у якому дезінформація використовується як інструмент стратегічного впливу. Прокремлівські інформаційні наративи спрямовані на маніпулювання громадською думкою, підрив морального стану суспільства та зменшення довіри до державних інституцій України. Широкомасштабні дезінформаційні кампанії російської федерації поєднують традиційні пропагандистські методи з новітніми технологіями впливу, зокрема кібератаками, інструментами штучного інтелекту та технологіями deepfake, що суттєво ускладнює їх своєчасне виявлення та нейтралізацію, особливо серед груп населення з низьким рівнем цифрової обізнаності.

Забезпечення інформаційної безпеки в банківській діяльності, шляхи попередження загроз і цілісність банківської інформації розглядали такі вітчизняні та зарубіжні вчені, як: Б. П. Адамик, О. І. Барановський, Ю. В. Ващенко, В. А. Гамза, І. Б. Заверуха, М. І. Зубок, І. С. Литвин, А. І. Марущак, Г. А. Нечай, Н. Ю. Пришва, І. Б. Ткачук, В. О. Ткачук, О. П. Орлюк, С. М. Побережний, Т. В. Субіна та інші. Але це питання потребує постійного вивчення, оскільки загрози в банківській сфері з кожним днем стрімко зростають.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Інформаційна безпека є невід'ємною складовою системи національної безпеки України та одним із ключових чинників забезпечення стійкості держави в умовах війни. Вона передбачає не лише захист інформаційного простору від зовнішніх загроз, а й розвиток внутрішньої здатності суспільства протидіяти інформаційним маніпуляціям. Для банківського сектору роль інформації має особливе значення, оскільки її достовірність, своєчасність і належний рівень захисту безпосередньо впливають на стабільність фінансової системи, рівень довіри клієнтів і партнерів, а також на загальний стан національної безпеки держави. Тому, незважаючи на існування наукових праць щодо інформаційної безпеки банків, ця тема залишається недостатньо вивченою на українському ринку.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є аналіз актуальних проблем і загроз у сфері інформаційної безпеки банківських установ, а також оцінка діючих механізмів захисту інформаційних ресурсів АТ «Сенс Банк» з подальшим формуванням практичних рекомендацій щодо підвищення їх ефективності.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Термін «інформаційна безпека» має різні тлумачення у працях науковців і в документах міжнародних організацій. У загальному розумінні інформаційну безпеку визначають як такий стан захищеності інформаційних ресурсів, за якого гарантується збереження їх конфіденційності, цілісності та доступності. У міжнародній практиці ці ключові характеристики відомі як тріада CIA (Confidentiality, Integrity, Availability).

Слід наголосити що, інформаційна безпека не обмежується лише протидією зовнішнім загрозам, а являє собою цілісну сукупність організаційних, технічних і правових заходів, спрямованих на забезпечення безперебійної та надійної діяльності банку в умовах цифровізації.

Казмірук Д. М. [1] зазначає, що попри наявність значної кількості наукових підходів до визначення поняття інформаційної безпеки, узгодженого трактування її сутності на сьогодні не сформовано. У межах свого дослідження автор акцентує увагу на позиції Гурковського В., відповідно до якої інформаційна безпека розглядається як сукупність суспільних відносин, спрямованих на захист життєво важливих інтересів особи, громадянина, суспільства та держави від наявних і потенційних загроз в інформаційному просторі. Такий захист виступає необхідною передумовою збереження й розвитку духовних і матеріальних цінностей нації, а також забезпечення існування, самозбереження та поступального розвитку України як суверенної держави [2].

Данильян О., Дзьобан О. та Панов М. розглядають інформаційну безпеку як стан захищеності об'єкта від загроз, що виникають у процесі обігу інформації, а також як систему заходів, спрямованих на збереження конфіденційності державної інформації [3].

Ліпкан В. пропонує багатовекторний підхід до розкриття змісту інформаційної безпеки, визначаючи її як захищеність інформаційного простору, процес протидії загрозам з метою забезпечення інформаційного суверенітету України, а також як механізм охорони національних інтересів у інформаційному середовищі [4].

Бондар І. тлумачить інформаційну безпеку як функціонування цілісної системи засобів і механізмів, що забезпечують захист інформаційних систем, до яких належать державні структури, фізичні та юридичні особи, а також програмно-технічні комплекси, що здійснюють автоматизовані інформаційні процеси, забезпечують дотримання прав людини та охорону інтересів суспільства і держави в інформаційній сфері [5].

Чинне законодавство України не містить вичерпного та чітко сформульованого визначення поняття інформаційної безпеки, однак у нормативно-правових актах вона розглядається як важлива складова системи національної безпеки. Такий підхід, зокрема, закріплено в Указі Президента України «Про Стратегію інформаційної безпеки», де інформаційна безпека України визначається як елемент національної безпеки, що відображає стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного устрою та інших життєво важливих інтересів особи, суспільства і держави.

Відповідно до зазначеного документа, за такого стану мають бути гарантовані конституційні права і свободи людини щодо збирання, зберігання, використання та поширення інформації, а також доступ до повної, достовірної й об'єктивної інформації. Водночас передбачається наявність ефективної системи захисту та протидії загрозам, пов'язаним із поширенням негативних інформаційних впливів, зокрема скоординованої дезінформації, деструктивної пропаганди, інших інформаційних операцій, а також несанкціонованого розповсюдження, використання чи порушення цілісності інформації з обмеженим доступом [6].

Так, у «Положенні про організацію системи внутрішнього контролю в банках України та банківських групах» інформаційна безпека – комплекс організаційних заходів банку, програмних і техніко-технологічних засобів, що функціонують на всіх організаційних рівнях банку та забезпечують захист інформації від випадкових та/або навмисних загроз, наслідком реалізації яких може стати порушення доступності, цілісності, конфіденційності інформації щодо діяльності банку або його клієнтів [7].

Положення про захист інформації та кіберзахист учасниками платіжного ринку розглядає інформаційну безпеку – як збереження конфіденційності, цілісності та доступності інформації [8].

Інший нормативний документ інформаційну безпеку трактує як стан захищеності, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та/або технологічних систем, конфіденційність, цілісність та доступність електронних інформаційних ресурсів, а також забезпечується своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз штатного режиму функціонування таких систем і ресурсів, несанкціонованого втручання в їх роботу [9].

За «Положенням про вимоги до системи управління кредитною спілкою» інформаційна безпека – комплекс організаційних заходів кредитної спілки, програмних і техніко-технологічних засобів, що функціонують на всіх організаційних рівнях кредитної спілки та забезпечують захист інформації від випадкових та/або навмисних загроз, наслідком реалізації яких може стати порушення доступності, цілісності, конфіденційності інформації щодо діяльності кредитної спілки або її клієнтів [10].

Ще законодавчо-нормативне регулювання захисту інформаційних ресурсів банківських установ представлено нормами Закону України «Про банки і банківську діяльність» і Закону України «Про інформацію». Окрім того в питаннях інформаційної безпеки банківських установ важливе місце займають і вимоги нормативно-правових актів НБУ з питань організації та управління інформаційною безпекою. Так, з метою підвищення рівня інформаційної безпеки установ банківської сфери з 2010 р. в Україні (відповідно до Постанови НБУ №474 від 28.10.2010р.) діють стандарти НБУ : СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності Система управління інформаційною безпекою. Вимоги» (ISO / IES 27001:2005, MOD); СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» (ISO / IES 27002:2005, MOD). Важливим документом є також «Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики

оцінки ризиків відповідно до стандартів Національного банку України від 01.03.2011р.». Ці методичні рекомендації розроблені на основі міжнародного стандарту ISO/IEC 27003:2010 з урахуванням особливостей банківської діяльності, стандартів та вимог Національного банку України з питань інформаційної безпеки.

На сьогодні в питаннях інформаційної безпеки прийняті, зокрема, такі міжнародні стандарти :

– серія ISO 27000 «Міжнародні стандарти для системи управління інформаційною безпекою» :

ISO/IEC 27000:2009. Визначення і основні принципи;

ISO/IEC 27001:2005. Інформаційні технології – Методики безпеки – Системи менеджменту інформаційної безпеки – Вимоги (BS 7799-2:2005);

ISO/IEC 27002:2005. Інформаційні технології – Методики безпеки – Практичні правила управління інформаційною безпекою;

ISO/IEC 27003:2010. Настанова з впровадження системи управління інформаційною безпекою; ISO/IEC 27005:2008. Інформаційні технології – Методика безпеки – Управління ризиками інформаційної безпеки (на основі стандарту BS 7799-3:2006);

ISO/IEC 27006:2007. Інформаційні технології – Методики безпеки – Вимоги до організації, що провадять аудит і сертифікацію систем менеджменту інформаційної безпеки;

ISO/IEC 27011:2008. Керівництво з менеджменту інформаційної безпеки для телекомунікацій;

ISO/IEC 15408. Загальні критерії оцінки безпеки інформаційних технологій;

– серія ISO 13335 «Міжнародні стандарти безпеки інформаційних технологій»:

ISO 13335-1:2004. Інформаційні технології – Керівництво по управлінню IT безпекою – Концепції і моделі для управління безпекою інформаційних і телекомунікаційних технологій;

ISO 13335-3:1998. Інформаційні технології – Керівництво по управлінню IT безпекою – Методи управління IT безпекою;

ISO 13335-4:2000. Інформаційні технології – Керівництво по управлінню IT безпекою – Вибір механізмів захисту; ISO 13335-5:2001. Інформаційні технології – Керівництво по управлінню IT безпекою – Керівництво по управлінню мережевою безпекою.

Досліджуючи питання інформаційної безпеки та інформаційної культури в умовах сучасного інформаційного суспільства, Панченко О. та Панченко Л. пропонують власне визначення інформаційної безпеки, а саме : інформаційна безпека характеризується як стан інформаційного середовища, що забезпечує задоволення інформаційних потреб учасників інформаційних відносин, охорону інформації та захист суб'єктів від негативного впливу інформації [11].

Інформаційну безпеку можна визначити як стан захищеності інформаційного середовища суспільства, який гарантує його формування, ефективне використання та розвиток у інтересах громадян, організацій і держави. Під інформаційним середовищем розуміється сукупність діяльності суб'єктів, пов'язаної зі створенням, обробкою та споживанням інформації.

Інформаційна безпека визначається як стан захищеності інформаційних потреб особи, суспільства та держави, за якого забезпечується їхнє існування та поступальний розвиток, незалежно від наявності внутрішніх чи зовнішніх загроз інформаційного характеру. Рівень інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої реальності, а отже, обґрунтованість ухвалюваних ними рішень та здійснюваних дій.

Інформаційна безпека виступає складовою національної безпеки та процесом управління загрозами й ризиками, здійснюваного державними й недержавними інституціями та окремими громадянами. Вона передбачає забезпечення :

– інформаційного суверенітету України;

– удосконалення державного регулювання розвитку інформаційної сфери, впровадження сучасних технологій у цій галузі та наповнення внутрішнього й міжнародного інформаційного простору достовірними даними про Україну;

– активного залучення засобів масової інформації до протидії корупції, зловживанням владою та іншим явищам, що становлять загрозу національній безпеці;

– неухильного дотримання конституційного права громадян на свободу слова та доступ до інформації, запобігання неправомірному втручанню органів державної влади й місцевого самоврядування у діяльність ЗМІ, дискримінації в інформаційній сфері та переслідуванню журналістів за їхні політичні переконання;

– здійснення комплексних заходів із захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

В контексті інформаційного права інформаційна безпека розглядається як одна зі сторін інформаційних відносин у межах законодавства про інформацію, зосереджуючи увагу на захисті життєво важливих інтересів особистості, суспільства та держави. Вона передбачає виявлення загроз цим інтересам та застосування правових механізмів для їх усунення або запобігання. Інформаційна безпека характеризує стабільний і стійкий стан системи, здатної зберігати ключові властивості для свого функціонування під впливом внутрішніх і зовнішніх загроз.

Отже, *основними характеристиками інформаційної безпеки* є:

Конфіденційність – недопущення несанкціонованого доступу до інформації сторонніми особами. У банківській діяльності це забезпечує гарантію того, що дані клієнтів, умови угод та внутрішні операції залишаються доступними лише для уповноважених користувачів.

Цілісність передбачає збереження повноти та достовірності інформації. У банківській сфері будь-які несанкціоновані або випадкові зміни у даних (наприклад, у платіжних документах, базах клієнтів або бухгалтерській звітності) можуть призвести до значних фінансових втрат та підірвати довіру до установи.

Доступність означає, що інформація та системи, у яких вона обробляється, повинні бути доступні користувачам у потрібний момент. Для банків це особливо важливо, оскільки навіть короткочасна недоступність інформаційних систем (інтернет-банкінгу, платіжних терміналів, мобільних додатків) може спричинити фінансові збитки та невдоволення клієнтів.

Для банківських установ інформаційна безпека має критичне значення з кількох причин :

1. *фінансовий аспект.* Будь-яке порушення захисту інформації може спричинити прямі фінансові збитки. За даними статистики, середні втрати від одного інциденту у фінансовому секторі значно перевищують аналогічні показники в інших галузях економіки.

2. *репутаційний аспект.* Довіра клієнтів до банку ґрунтується на гарантії збереження їхніх коштів та персональних даних. Витік конфіденційної інформації або успішна кібератака миттєво призводять до зниження рівня довіри та відтоку клієнтів.

3. *правовий аспект.* Банки зобов'язані забезпечувати захист персональних даних клієнтів і дотримуватися вимог законодавства України, а також міжнародних регламентів, таких як GDPR.

4. *національний аспект.* Банківська система є частиною критичної інфраструктури держави, тому масові атаки на банки можуть викликати дестабілізацію економіки та соціальної сфери.

Отже, інформаційна безпека в банку є не вузькоспеціалізованим завданням IT-відділу, а комплексною корпоративною функцією, що інтегрується у всі бізнес-процеси установи.

Розвиток інформаційних технологій істотно змінив підхід до інформаційної безпеки :

– 1990-ті роки : акцент робився на технічних засобах захисту, таких як антивірусні програми, міжмережеві екрани та фізична охорона серверів.

– Початок 2000-х : зростає значення організаційних заходів — розробка політик доступу, аудит інформаційних систем, стандартизація процедур.

– 2010-ті роки : інформаційна безпека інтегрується у бізнес-моделі банків, формуються підходи до управління інформаційними ризиками.

– 2020 – 2025 роки : банки впроваджують комплексні моделі кіберзахисту, що поєднують технічні засоби, нормативні процедури та людський фактор. Особлива увага приділяється стратегіям Zero Trust, багатофакторній автентифікації та використанню штучного інтелекту для виявлення аномалій.

Сучасна інформаційна безпека в банку має розглядатися як система заходів, що включає:

– правові заходи : дотримання законодавства та внутрішніх регламентів;

– організаційні заходи : розмежування доступу, контроль дій персоналу, впровадження політик безпеки;

– технічні заходи : шифрування даних, захищені канали передачі, системи виявлення вторгнень;

– кадрові заходи : навчання співробітників та протидія соціальній інженерії;

– управлінські заходи : інтеграція інформаційної безпеки у стратегію розвитку банку та управління ризиками.

Лише за умови взаємодії всіх цих елементів можливо сформувати ефективну систему захисту, здатну протистояти сучасним викликам.

Зі збільшенням популярності інтернет-банкінгу, мобільних додатків та платіжних сервісів зростає кількість каналів доступу до банківських ресурсів, що, своєю чергою, розширює можливі шляхи для атак.

Клієнти очікують від банку високого рівня зручності у користуванні послугами, водночас вимагаючи надійного захисту своїх даних. Це створює ключове завдання: поєднати простоту доступу з максимальною безпекою. У цьому контексті обов'язковим стає застосування двофакторної та багатофакторної автентифікації, біометричних технологій і поведінкової аналітики.

Цифрова трансформація також породжує нові загрози — від атак на мобільні додатки до ризиків у сфері відкритого банкінгу (Open Banking). Це змушує банки переходити до проактивного підходу : передбачати потенційні інциденти, використовуючи інтелектуальний аналіз даних та автоматизовані системи моніторингу, а не лише реагувати на них.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Таким чином, інформаційна безпека в банківській сфері є багатогранним явищем, що включає технічні, організаційні, правові та соціальні складові. Її сутність полягає не тільки у захисті даних від зловмисників, а й у створенні умов для стабільного функціонування банку в цифровому середовищі, забезпечуючи клієнтам безпеку їх фінансових ресурсів і персональної інформації.

Сьогодні інформаційна безпека є ключовим фактором довіри до банку та його конкурентоспроможності. Вона повинна розглядатися не як витратна стаття, а як стратегічна інвестиція, що гарантує стійкість і розвиток банківської установи у майбутньому. Забезпечення інформаційної безпеки банківських установ є нагальною і актуальною проблемою їх функціонування і розвитку, адже несе у собі потенціал збереження і ефективного використання фінансових, матеріальних та інформаційних ресурсів банків, своєчасного виявлення та нейтралізації реальних та потенційних загроз, а також формування умов реалізації банками своїх стратегічних інтересів.

Література

1. Казмірук Д. М. Інформаційна безпека як складова національної безпеки в умовах повномасштабної війни. Науковий журнал «Політикус». 2025. Вип. 1. С. 21 – 26. https://doi.org/10.24195/2414- 9616.2025-1.3

2. Гурковський В. І. Безпека як об'єкт правовідносин в умовах глобального інформаційного суспільства. *Правова інформатика.* 2010. № 2 (26). С. 72 – 77.

3. Данильян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України : структура та напрямки реалізації : навчальний посібник. Харків : Фоліо, 2002. 285 с.

4. Ліпкан В. А., Харченко Л. С., Логінов О. В. Інформаційна безпека України : Глосарій. Київ : Текст, 2004. 136 с.

5. Бондар І. Р. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation*. 2014. № 1. С. 68 – 75.

6. Указ Президента України від 28.12.2021 р., № 685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL : https://zakon.rada.gov.ua/laws/show/685/2021#Text

7. Постанова Національного банку України від 02.07.2019 р., № 88 «Про затвердження Положення про організацію системи внутрішнього контролю в банках України та банківських групах». URL : https://zakon.rada.gov.ua/laws/show/v0088500-19#Text

8. Постанова Національного банку України від 19.05.2021 р., № 43 «Про затвердження Положення про захист інформації та кіберзахист учасниками платіжного ринку». URL : https://zakon.rada.gov.ua/laws/show/v0043500-21#Text

9. Постанова Кабінету Міністрів України від 24.03.2023 р., № 257 «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури». URL : https://zakon.rada.gov.ua/laws/show/257-2023-%D0%BF#Text

10. Постанова Національного банку України від 02.02.2024 р., № 15 «Про затвердження Положення про вимоги до системи управління кредитною спілкою». URL : https://zakon.rada.gov.ua/laws/show/v0015500-24#Text

11. Панченко О. А., Панченко Л. В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. *Правова інформатика*. 2015. № 2(46). С. 32 – 38.

References

1. Kazmiruk D. M. (2025). Informatsiina bezpeka yak skladova natsionalnoi bezpeky v umovakh povnomasshtabnoi viiny. [Information security as a component of national security in conditions of full-scale war.]. Naukovyi zhurnal «Politykus». [Scientific journal «Politicus».]. Vyp. 1. Pp. 21 – 26. https://doi.org/10.24195/2414- 9616.2025-1.3 (in Ukraine).

2. Hurkovskyi V. I. (2010). Bezpeka yak obiekt pravovidnosyn v umovakh hlobalnoho informatsiinoho suspilstva. [Security as an object of legal relations in the conditions of a global information society.]. Pravova informatyka. [Legal informatics.]. № 2 (26). Pp. 72 – 77. (in Ukraine).

3. Danylian O. H., Dzoban O. P., Panov M. I. (2002). Natsionalna bezpeka Ukrainy : struktura ta napriamky realizatsii : navchalnyi posibnyk. [National security of Ukraine : structure and directions of implementation : textbook.]. Kharkiv : Folio. 285 p. (in Ukraine).

4. Lipkan V. A., Kharchenko L. S., Lohinov O. V. (2004). Informatsiina bezpeka Ukrainy : Hlosarii. [Information security of Ukraine : Glossary.]. Kyiv : Tekst. 136 p. (in Ukraine).

5. Bondar I. R. (2014). Informatsiina bezpeka yak osnova natsionalnoi bezpeky. [Information security as the basis of national security..]. Mekhanizm ekonomichnoho rehuliuvannia. [Mechanism of Economic Regulation]. № 1. Pp. 68 – 75. (in Ukraine).

6. Ukaz Prezydenta Ukrainy vid 28.12.2021 r., № 685/2021 «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky». [On the decision of the National Security and Defense Council of Ukraine of October 15, 2021 «On the Information Security Strategy»]. URL : https://zakon.rada.gov.ua/laws/show/685/2021#Text (in Ukraine).

7. Postanova Natsionalnoho banku Ukrainy vid 02.07.2019 r., № 88. «Pro zatverdzhennia Polozhennia pro orhanizatsiiu systemy vnutrishnoho kontroliu v bankakh Ukrainy ta bankivskykh hrupakh». [On approval of the Regulation on the organization of the internal control system in Ukrainian banks and banking groups]. URL : https://zakon.rada.gov.ua/laws/show/v0088500-19#Text(in Ukraine).

8. Postanova Natsionalnoho banku Ukrainy vid 19.05.2021 r., № 43 «Pro zatverdzhennia Polozhennia pro zakhyst informatsii ta kiberzakhyst uchasnykamy platizhnoho rynku». [On approval of the Regulation on information protection and cyber security by payment market participants.]. URL : https://zakon.rada.gov.ua/laws/show/v0043500-21#Text (in Ukraine).

9. Postanova Kabinetu Ministriv Ukrainy vid 24.03.2023 r., № 257 «Deiaki pytannia provedennia nezalezhnoho audytu informatsiinoi bezpeky na obiektakh krytychnoi infrastruktury». [Some issues of conducting an independent audit of information security at critical infrastructure facilities.]. URL : https://zakon.rada.gov.ua/laws/show/257-2023-%D0%BF#Text (in Ukraine).

10. Postanova Natsionalnoho banku Ukrainy vid 02.02.2024 r., № 15 «Pro zatverdzhennia Polozhennia pro vymohy do systemy upravlinnia kredytnoiu spilkoiu». [On approval of the Regulation on requirements for the credit union management system.]. URL : https://zakon.rada.gov.ua/laws/show/v0015500-24#Text (in Ukraine).

11. Panchenko O. A., Panchenko L. V. (2015). Informatsiina bezpeka ta informatsiina kultura v suchasnomu informatsiinomu suspilstvi. [Information security and information culture in the modern information society.]. Pravova informatyka. [Legal informatics.]. № 2(46). Pp. 32 – 38. (in Ukraine).