DOI 10.36074/grail-of-science.15.05.2026.066

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ: СУЧАСНІ ПІДХОДИ ТА ІНСТРУМЕНТИ

Кравчук Ірина Миколаївна
доктор філософії, доцент, доцент кафедри логістики та підприємництва
Луцький національний технічний університет, Україна

Анотація. *У статті досліджено сучасні підходи та інструменти управління інформаційною безпекою суб'єктів господарювання в умовах цифровізації економіки, зростання обсягів електронного документообігу, активного використання хмарних сервісів, автоматизованих систем управління та онлайн-комунікацій. Обґрунтовано, що інформаційна безпека є не лише технічним напрямом захисту даних, а й важливою складовою загальної системи економічної безпеки підприємства, оскільки безпосередньо впливає на стабільність бізнес-процесів, збереження комерційної таємниці, репутацію, конкурентоспроможність і довіру партнерів та клієнтів. У межах дослідження визначено основні загрози інформаційній безпеці суб'єктів господарювання, серед яких особливе місце займають несанкціонований доступ до конфіденційної інформації, витік персональних даних, фішингові атаки, шкідливе програмне забезпечення, кібер-шахрайство, людський фактор, недостатній рівень цифрової грамотності персоналу та відсутність системного контролю за інформаційними потоками. Розглянуто організаційні, технічні, правові та економічні інструменти забезпечення інформаційної безпеки, зокрема політику доступу до інформаційних ресурсів, резервне копіювання даних, використання антивірусного захисту, багатофакторну автентифікацію, внутрішній аудит, навчання працівників, регламентацію роботи з конфіденційною інформацією та оцінювання інформаційних ризиків. Зроблено висновок, що ефективне управління інформаційною безпекою суб'єктів господарювання потребує комплексного, ризик-орієнтованого та безперервного підходу. Запропоновано розглядати інформаційну безпеку як стратегічний управлінський процес, що має бути інтегрований у загальну систему менеджменту підприємства та адаптований до масштабу діяльності, галузевої специфіки, ресурсних можливостей і рівня цифрової зрілості суб'єкта господарювання.*

Ключові слова: *інформаційна безпека; суб'єкти господарювання; управління інформаційними ризиками; цифровізація бізнесу.*

Постановка проблеми. У сучасній економіці інформація перетворилася на один із ключових ресурсів підприємницької діяльності. Вона забезпечує прийняття управлінських рішень, організацію виробничих, фінансових, логістичних і маркетингових процесів, взаємодію з клієнтами, постачальниками та державними органами. Водночас інформаційні ресурси дедалі частіше стають об'єктом неправомірного доступу, знищення, блокування, підміни або

комерційного використання третіми особами. Для підприємства це означає не лише технічні втрати, а й економічні наслідки: простій бізнес-процесів, втрату клієнтської довіри, репутаційні ризики, штрафні санкції та послаблення конкурентних позицій.

Актуальність проблеми посилюється цифровізацією бізнесу. Електронний документообіг, ERP- і CRM-системи, онлайн-банкінг, хмарні сервіси, дистанційна робота, маркетплейси й мобільні застосунки створюють значні переваги, але одночасно розширюють зону вразливості. У таких умовах підприємство вже не може обмежитися лише антивірусним програмним забезпеченням або разовими технічними заходами. Інформаційна безпека потребує системного управління, чіткого розподілу відповідальності, контролю доступу, навчання персоналу, аудиту та постійного вдосконалення.

Для українських суб'єктів господарювання проблема має також кризовий вимір, зумовлений воєнними ризиками, кібератаками, фішинговими кампаніями та залежністю бізнесу від цифрових сервісів. Саме тому інформаційну безпеку доцільно розглядати не як допоміжну функцію IT-відділу, а як складову стратегічного управління підприємством.

Аналіз досліджень та публікацій. Аналіз наукових досліджень свідчить про значну увагу вітчизняних і зарубіжних учених до формування концептуальних засад системи управління інформаційною безпекою. Зокрема, у працях Ковальської Л.Л. розкривається сутність інформаційної безпеки як комплексної категорії, що охоплює не лише технічні аспекти захисту інформації, а й організаційні, економічні та правові механізми забезпечення безпеки підприємства. Дослідниця акцентує увагу на необхідності інтеграції системи інформаційної безпеки в загальну систему управління підприємством, що забезпечує узгодженість стратегічних і операційних рішень.

У наукових роботах Білька С., Дубницького В., значна увага приділяється ризик-орієнтованому підходу до управління інформаційною безпекою. Автори обґрунтовують доцільність використання інструментів ідентифікації, оцінювання та ранжування інформаційних ризиків, зокрема через застосування карт ризиків та матричних моделей. При цьому підкреслюється, що ефективність системи безпеки безпосередньо залежить від здатності підприємства своєчасно виявляти загрози та адаптуватися до змін зовнішнього середовища.

Мета роботи. Метою статті є наукове обґрунтування сучасних підходів та інструментів управління інформаційною безпекою суб'єктів господарювання, а також формування практичної моделі, що може бути використана підприємствами для ідентифікації інформаційних ризиків, захисту критичних активів, реагування на інциденти та підвищення стійкості бізнес-процесів.

Досягнення визначеної мети передбачає уточнення сутності інформаційної безпеки, систематизацію основних загроз, характеристику організаційних, технічних, правових, економічних та освітніх інструментів, побудову ризик-орієнтованої моделі управління інформаційною безпекою.

Виклад основного матеріалу. Інформаційна безпека суб'єкта господарювання – це стан захищеності інформаційних ресурсів, інформаційних систем, каналів комунікації, управлінських процесів і ділової репутації від

внутрішніх і зовнішніх загроз, що можуть призвести до порушення конфіденційності, цілісності або доступності інформації.

Управління інформаційною безпекою доцільно розглядати як безперервний процес, який охоплює визначення інформаційних активів, оцінювання ризиків, вибір захисних заходів, впровадження політик і технічних контролів, моніторинг, аудит, реагування на інциденти та вдосконалення системи. Такий підхід дає змогу перейти від фрагментарного захисту до системного управління (рис. 1). Як показано на рис. 1, управління інформаційною безпекою має циклічний характер.

У центрі схеми розміщено ключове поняття – цикл управління інформаційною безпекою, що підкреслює системний характер цього процесу та його спрямованість на забезпечення конфіденційності, цілісності й доступності інформації. Такий підхід відповідає сучасному розумінню інформаційної безпеки як складової загальної системи управління підприємством, а не лише як сукупності технічних заходів захисту.

Рис. 1. Цикл управління інформаційною безпекою суб'єкта господарювання

Сформовано автором на основі джерел [1,2,5,6]

Рисунок відображає системний та безперервний характер управління інформаційною безпекою підприємства у вигляді замкненого циклу. У центрі схеми акцентовано ключову мету – забезпечення конфіденційності, цілісності та доступності інформації. Перший етап передбачає встановлення контексту та

планування, що включає визначення цілей, політики та ресурсів. Наступні етапи охоплюють ідентифікацію та оцінювання ризиків, а також вибір і впровадження заходів їх мінімізації. Важливими складовими є експлуатація системи безпеки, моніторинг її ефективності та аналіз результатів. Завершальний етап передбачає перегляд і постійне вдосконалення системи, що забезпечує її адаптацію до змін середовища.

У сучасних умовах цифровізації діяльності підприємств зростає значущість ефективного управління інформаційними ризиками як складової забезпечення їх економічної безпеки. Одним із інструментів систематизації та оцінювання таких ризиків є карта інформаційних ризиків, яка дозволяє візуалізувати рівень загроз залежно від їх ймовірності та впливу на діяльність суб'єкта господарювання представлено на рис. 2.

Рис. 2. Приклад карти інформаційних ризиків підприємства

Сформовано автором на основі джерел [1,2,3,4]

Рисунок демонструє карту інформаційних ризиків у вигляді матриці, що поєднує оцінку ймовірності та впливу ризиків. По горизонталі відображено рівень ймовірності виникнення загроз, а по вертикалі — рівень їх впливу на діяльність підприємства. Кольорова диференціація дозволяє швидко визначити рівень ризику: від низького до критичного. У правій частині подано перелік основних інформаційних ризиків із їх кількісною оцінкою та категоризацією. Найбільш небезпечними визначено кібератаки та витік конфіденційної інформації, які мають критичний рівень. Карта ризиків слугує інструментом для визначення пріоритетів управління та прийняття обґрунтованих рішень щодо захисту інформації. Отже, карта інформаційних ризиків є ефективним інструментом візуалізації стану інформаційної безпеки підприємства. Вона дозволяє систематизувати ризики, визначити їхню пріоритетність, обрати

адекватні заходи реагування та забезпечити контроль за динамікою ризикового середовища. У поєднанні з циклом управління інформаційною безпекою така карта може використовуватися як практична основа для формування політики інформаційної безпеки, планування захисних заходів і підвищення стійкості підприємства до інформаційних загроз. Ефективна інформаційна безпека не може забезпечуватися лише однією групою інструментів. Технічний захист без політик і контролю не гарантує належного рівня безпеки, а правові документи без реальних процедур залишаються формальними. Тому підприємство має поєднувати різні інструменти в єдину систему [5].

Організаційні інструменти формують основу управління. До них належать політика інформаційної безпеки, порядок використання корпоративної електронної пошти, правила зберігання документів, порядок реагування на інциденти та інструкції щодо роботи з хмарними сервісами. Технічні інструменти забезпечують безпосередній захист інформаційних систем: MFA, оновлення програм, антивірусний захист, резервне копіювання, шифрування, контроль доступу та моніторинг підозрілої активності.

Правові інструменти необхідні для захисту інтересів підприємства у відносинах із працівниками, клієнтами, партнерами та постачальниками. Економічні інструменти дають змогу оцінити можливі збитки та обґрунтувати інвестиції в захист. Наступним етапом є оцінювання ризиків. Для кожного критичного активу встановлюються можливі загрози, наявні вразливості, імовірність інциденту та потенційні наслідки. Після цього розробляється план захисних заходів: оновлення програмного забезпечення, обмеження адміністративних прав, резервне копіювання, перевірка договорів із постачальниками цифрових послуг і проведення навчання працівників.

Важливим елементом управління є моніторинг і реагування на інциденти. Підприємство повинно мати зрозумілий порядок дій у разі втрати доступу, зараження комп'ютера, витоку інформації або компрометації облікового запису. Для суб'єктів малого і середнього підприємництва доцільним є поетапне впровадження інформаційної безпеки

Висновки та пропозиції. У результаті дослідження встановлено, що інформаційна безпека суб'єктів господарювання є важливою складовою економічної безпеки підприємства і безпосередньо впливає на стабільність, конкурентоспроможність, ділову репутацію та безперервність бізнес-процесів. В умовах цифровізації інформаційні ризики набувають системного характеру, тому потребують не фрагментарного технічного захисту, а комплексного управлінського підходу.

Обґрунтовано, що сучасна система управління інформаційною безпекою повинна будуватися на принципах ризик-орієнтованості, безперервності, відповідальності керівництва, інтеграції в загальну систему менеджменту, правової визначеності, економічної доцільності та залучення персоналу. Найбільш результативним є поєднання організаційних, технічних, правових, економічних та освітніх інструментів.

Список використаних джерел:

[1] Білько С. Інформаційна та економічна безпека: оцінювання рівня та взаємозв'язку. Науковий вісник. Полісся. 2022. 1 (24), С. 58–77.

[2] Дубницький В.І., Науменко Н.Ю. Методологічне забезпечення формування інформаційної безпеки в сфері економічної безпеки регіону. Вісник економічної науки України. 2019. №1. URL: http://dspace.nbuv.gov.ua/handle/123456789/151638 (дата звернення: 07.04.2026).

[3] Краус К.М., Краус Н.М., Штепа О.В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. Innovation and Sustainability. 2022. № 3. С. 26–37.

[4] Ковальська Л., Топалов В., Топалов Р. Інформаційна безпека регіону: підходи до розгляду та економічна сутність. Економічний форум. 2023. № 13 (2), С. 18–24.

[5] Кузьомко В. Інформаційна безпека бізнесу в умовах цифрової трансформації економіки. Інноваційне підприємництво: стан та перспективи розвитку: збірник матеріалів VI Всеукраїнської науково-практичної конференції (м. Київ, 29-30.03.2021). Київ: КНЕУ. 2021. С. 26–28.

[6] Шостак Л., Помазун О. Інформаційна безпека в контексті інноваційного розвитку бізнес-моделі вітчизняних підприємств в умовах цифрової економіки. Цифрова економіка та економічна безпека. 2024. № 5 (14), С. 160–165.

[7] Bilko S. (2022). Informatsiina ta ekonomichna bezpeka: otsiniuvannia rivnia ta vzaiemozviazku [Information and economic security: assessment of level and interconnection]. Naukovyi visnyk Polissia, 1 (24), pp. 58–77. (in Ukrainian).

[8] Dubnytskyi V.I., Naumenko N.Yu. (2019). Metodolohichne zabezpechennia formuvannia informatsiinoi bezpeky v sferi ekonomichnoi bezpeky rehionu [Methodological support for the formation of information security in the field of regional economic security]. Visnyk ekonomichnoi nauky Ukrainy, (1). Retrieved from http://dspace.nbuv.gov.ua/ handle/123456789/151638 (accessed: May 2, 2026). (in Ukrainian).

[9] Kraus K.M., Kraus N.M., Shtepa O.V. (2022). Tsyfrova transformatsiia kiberbezpeky na mikroriavni v umovakh voiennoho stanu [Digital transformation of cybersecurity at the micro level under martial law]. Innovation and Sustainability, (3), pp. 26–37. (in Ukrainian).

[10] Kovalska L., Topalov V., Topalov R. (2023). Informatsiina bezpeka rehionu: pidkhody do rozghliadu ta ekonomichna sutnist [Regional information security: approaches and economic essence]. Ekonomichnyi forum, 13 (2), pp. 18–24. (in Ukrainian).

[11] Kuziomko V. (2021). Informatsiina bezpeka biznesu v umovakh tsyfrovykh transformatsii ekonomiky [Information security of business in conditions of digital transformation of the economy]. In Innovatsiine pidpryiemnytstvo: stan ta perspektyvy rozvytku (pp. 26–28). Kyiv: KNEU. (in Ukrainian).

[12] Shostak L., Pomazun O. (2024). Informatsiina bezpeka v konteksti innovatsiinoho rozvytku biznes-modeli vitchyznianykh pidpryiemstv v umovakh tsyfrovoi ekonomiky [Information security in the context of innovative development of domestic business models under digital economy]. Tsyfrova ekonomika ta ekonomichna bezpeka, 5 (14), pp. 160–165. (in Ukrainian).

INFORMATION SECURITY MANAGEMENT OF BUSINESS ENTITIES: MODERN APPROACHES AND TOOLS

Iryna Kravchuk
Doctor of Philosophy, Associate Professor,
Associate Professor of the Department of Logistics and Entrepreneurship
Lutsk National Technical University, Ukraine
ORCID ID: 0000-0001-8291-3943

Summary. *The article examines modern approaches and tools for managing information security of business entities in the context of economic digitalization, the growing volume of electronic document flow, the active use of cloud services, automated management systems, and online communications. It is substantiated that information security is not only a technical area of data protection but also an important component of the*

overall system of an enterprise's economic security, as it directly affects the stability of business processes, the preservation of trade secrets, reputation, competitiveness, and the trust of partners and customers. The study identifies the main threats to the information security of business entities, among which unauthorized access to confidential information, leakage of personal data, phishing attacks, malware, cyber fraud, the human factor, insufficient digital literacy of personnel, and the absence of systematic control over information flows occupy a special place. The article considers organizational, technical, legal, and economic tools for ensuring information security, in particular access policies for information resources, data backup, the use of antivirus protection, multi-factor authentication, internal audit, employee training, regulation of work with confidential information, and assessment of information risks. It is concluded that effective management of information security of business entities requires a comprehensive, risk-oriented, and continuous approach. Information security is proposed to be regarded as a strategic management process that should be integrated into the overall enterprise management system and adapted to the scale of activity, industry-specific features, resource capabilities, and level of digital maturity of a business entity.

Keywords: *information security; business entities; information risk management; business digitalization.*

Дата публікації: 15.05.2026

Дата першого надходження статті до видання: 06.04.2026
Дата прийняття статті до друку після рецензування: 30.04.2026