DOI: https://doi.org/10.32782/2524-0072/2024-61-66

УДК 658

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ТА ЙОГО УДОСКОНАЛЕННЯ

INFORMATION SECURITY OF MANAGEMENT OF THE SYSTEM OF ECONOMIC SECURITY OF THE ENTERPRISE AND ITS IMPROVEMENT"

Мачак Тетяна Олександрівна
старший викладач,
Дніпровський державний аграрно-економічний університет
ORCID: https://orcid.org/0000-0002-3746-4736

Дубина Олена Леонідівна
старший викладач,
Дніпровський державний аграрно-економічний університет
ORCID: https://orcid.org/0000-0002-3707-2281

Юрченко Сергій Васильович
кандидат економічних наук, доцент,
Дніпровський державний аграрно-економічний університет
ORCID: https://orcid.org/0000-0001-5148-2626

Machak Tatiana, Dubyna Olena, Yurchenko Sergey
Dnipro State Agrarian and Economic University

Стаття присвячена актуальним питанням забезпечення інформаційної безпеки як важливої складової фінансово-економічної безпеки підприємства. Розглядається значення та роль інформаційної безпеки в загальній системі фінансово-економічної безпеки підприємства, а також основні фактори, що впливають на неї. Детально розглянуто і проаналізовано класифікаційні ознаки, що допомагають визначати основні джерела загроз інформаційній безпеці підприємства. На основі цього аналізу розроблено комплексний план заходів з інформаційної безпеки, спрямований на прогнозування потенційних ризиків і вжиття відповідних профілактичних заходів для мінімізації можливих збитків. Визначено, що ефективна реалізація цього плану потребує постійного моніторингу та адаптації до змін у сфері інформаційної безпеки, а також активної участі керівництва та всіх працівників підприємства у процесі забезпечення інформаційної безпеки.

Ключові слова: економічна безпека, інформаційна безпека, управління безпекою, захист інформації, забезпечення інформаційної безпеки.

The article is devoted to topical issues of ensuring information security as an important component of the financial and economic security of the enterprise. It was determined that information security is a structural element of the company's financial and economic security system. The importance of information security in the system of financial and economic security is determined by its role in protecting confidential information, ensuring the integrity and availability of data, as well as in maintaining the stability of financial processes. The main factors affecting information security have been identified. The classification features that help to determine the main sources of threats to the information security of the enterprise are considered and analyzed in detail. Depending on the criteria, threats to information security are divided depending on the sources of formation, by the method of occurrence, by methods of countering threats, and others. The types of damage that threats can cause are considered, among which financial and reputational consequences are distinguished. Based on this analysis, a comprehensive plan for ensuring the information security of the enterprise has been developed, aimed at predicting potential risks and applying appropriate preventive measures to eliminate them and minimize possible losses. In addition, it is noted that the successful implementation of this plan requires constant monitoring and adaptation to changes in the field of information security, as well as the development of a recovery strategy after the occurrence of possible incidents. This strategy includes a number of practices aimed at effectively restoring business processes and recovering data

in the event of an incident. It was emphasized that the active participation of management and all employees of the enterprise, especially accountants, in ensuring information security is crucial for the successful implementation of the plan. Such a comprehensive approach will allow the enterprise to effectively respond to modern challenges in the field of information security and ensure the stability and efficiency of the general system of financial and economic security of the enterprise.

Keywords: economic security, information security, security management, information protection, ensuring information security.

Постановка проблеми. Сьогоднішні реалії свідчать, що вагомий вплив на безпеку підприємств має інформаційна складова економічної безпеки. Це пояснюється тим, що в сучасному світі обмін інформацією став ключовим елементом економічної діяльності. Розвиток інформаційних технологій, автоматизація робочих місць, введення електронного документообігу та ряд інших чинників сприяють ефективному використанню як людських так і матеріальних ресурсів. Поряд з цим у підприємств виникає залежність від інформаційних технологій при виробництві продукції, маркетингу, обслуговування клієнтів та інших аспектів свого бізнесу. Це створює унікальні виклики і загрози, такі як кібератаки, витоки даних та інші форми кіберзлочинності, які можуть серйозно підірвати довіру клієнтів, призвести до фінансових втрат і пошкодити репутацію компанії. Таким чином, забезпечення безпеки інформації є необхідною умовою для забезпечення економічної безпеки підприємства та успішної діяльності будь-якого сучасного підприємства

Аналіз останніх досліджень і публікацій. Вагомий вклад у формування та розвиток питань забезпечення економічної безпеки зроблено такими науковцями, як: Архіпов О., Шевчук М. О., Захаров О. І., Гнатенко В., Іванченко Н. О., Жуків А., Бєляєв А. та інші. Важливість їх праць полягає в уточненні та поглибленні розуміння принципів забезпечення захисту інформації в сучасному цифровому середовищі.

Формулювання цілей статті (постановка завдання). Мета дослідження є розгляд основних аспектів поняття інформаційна безпека та пошук напрямів удосконалення інформаційного забезпечення управління системою економічної безпеки підприємства.

Виклад основного матеріалу дослідження. Економічна безпека являється важливим елементом успіху і стабільності підприємств і залежить від здатності керівників вчасно реагувати на потенційні загрози та швидко адаптуватися до змін в економічному середовищі. При цьому, кожна складова економічної безпеки, включаючи фінансову, правову, кадрову, технологічну та інформаційну, має свою вагу і впливає на загальний стан підприємства. Досліджуючи структуру економічної безпеки, важливо враховувати, що всі компоненти взаємопов'язані між собою і є основою для стабільного розвитку підприємства (рис. 1).

Кожна з цих складових є важливою для забезпечення ефективності економічної безпеки підприємства. Взаємодія між ними і формування комплексного підходу дозволяє підприємству оптимізувати свою діяльність, зменшити ризики та забезпечити стійкість у складних умовах ринкової конкуренції.

Основною передумовою ефективного управління компанією є удосконалення системи інформаційного забезпечення.

В законодавстві України, питання інформаційної безпеки знайшли своє відображення у Законі України "Про основні принципи розвитку інформаційного суспільства в Україні на період 2007–2015 років", в якому визначено поняття «інформаційна безпека» як: «Стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [1].

Звертаємо увагу на те, поняття «інформаційна безпека» давно відоме та знаходить широке застосування у наукових статтях, навчальних матеріалах та нормативно-правових актах різного рівня, однак тлумачення цього терміну продовжує залишатися неоднозначним.

Так, наприклад, Гнатенко В. вважає, що «інформаційна безпека» – це: «Стан інформаційного середовища, що забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації і захист суб'єктів від негативної інформаційної дії» [3].

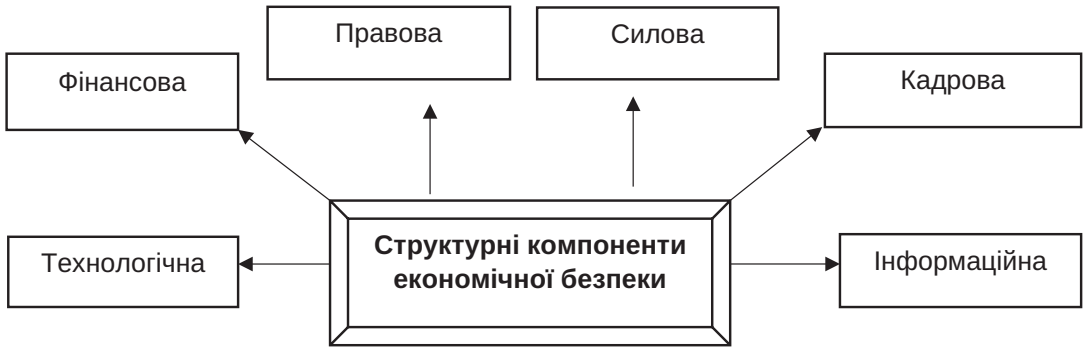

Рис. 1. Структурні компоненти економічної безпеки підприємства

Джерело: сформовано на основі [1]

Архипов О., пропонує інший погляд на трактування «інформаційної безпеки», визначаючи її як: «Поточний стан захищеності об'єкта від інформаційних загроз, який визначається рівнем шкоди, що може бути заподіяна діяльності об'єкта в разі реалізації загроз», а саме: «Використання неповної, несвоєчасної і недостовірної інформації; здійснення негативного інформаційного впливу; протиправного застосування інформаційних технологій; несанкціонованого розповсюдження і використання інформації, порушення її цілісності, конфіденційності та доступності» [2].

Схоже визначення відображено і в працях Захарова О. І. Автор вважає, що, «інформаційна безпека» – це: «Стан захищеності життєво важливих інтересів особи, суспільства і держави, при якому зводиться до мінімуму заподіяння шкоди через неповноту, несвоєчасність і недостовірність інформації, через негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації» [4]. В своєму підході автор окреслює рамки та напрямки захисту інформаційного простору країни і підприємств, підкреслюючи необхідність створення безпечного інформаційного середовища для громадян та організацій.

Шевчук М. О. вважає, що «інформаційна безпека» – це: «Стійкий стан інформаційної сфери, що забезпечує її цілісність і захищеність об'єктів за наявності негативних внутрішніх і зовнішніх впливів, заснований на усвідомленні людиною своїх цінностей, потреб і цілей розвитку» [6]. В основу цього поняття лягає усвідомлення людьми власних цінностей, життєво необхідних потреб і стратегічних цілей розвитку, що в сукупності формує міцний фундамент для забезпечення інформаційної безпеки.

Дослідивши різні підходи тлумачення даного поняття, можемо виділити основні концепції, наведені на рис. 2.

Наведені підходи демонструють багатогранність поняття інформаційної безпеки, її важливу роль у забезпеченні стабільності та розвитку держави. Водночас, вони підкреслюють необхідність комплексного підходу до забезпечення інформаційної безпеки.

Забезпечення інформаційної безпеки стає дедалі важливішим аспектом управління підприємством в сучасному світі. Швидкі темпи технологічного розвитку та поширення цифрових інструментів створюють нові можливості для бізнесу. Сучасні підприємства активно використовують передові технології та автоматизовані системи обліку для оптимізації своєї роботи та забезпечення конкурентоспроможності. Використання різних технічних засобів комунікації для передачі і зберігання інформації, перехід до автоматизованих систем обліку і документообігу, впровадження аналітичних систем для обробки даних – все це призводить до накопичення значного обсягу інформації, яка обробляється та зберігається для подальшого аналізу і використання. Зростаючий обсяг даних та його розміщення на цифрових носіях створює нові загрози безпеки інформації. Тому, важливо створити умови для забезпечення збереження інформації, щоб запобігти її витоку, викривлення, викрадення або знищення, особливо враховуючи конфіденційний характер інформаційних даних. Це вимагає від керівництва ретельного планування, постійного моніторингу та готовності до оперативного реагування на можливі загрози.

Загрози інформаційній безпеці охоплюють усі наявні та потенційні чинники, які можуть створювати небезпеку і загрожувати інтересам підприємства у різних сферах діяль-

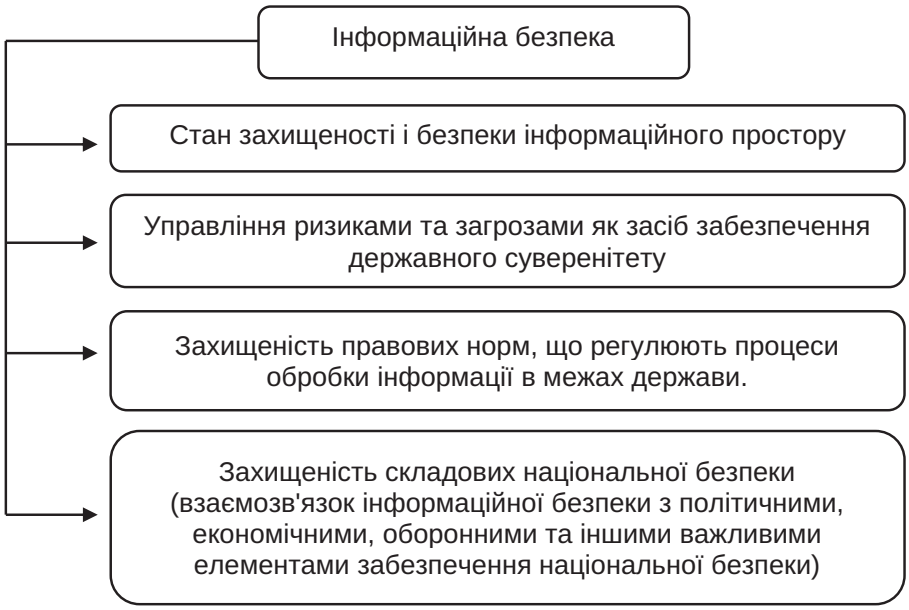

Рис. 2. Підходи до сутності поняття «інформаційна безпека»

Джерело: сформовано авторами на основі [2–6]

ності. Основою ефективного захисту є глибоке розуміння різноманітності загроз, які можуть виникнути, та методів їх класифікації. Залежно від критеріїв, можливо виділити різні підходи до розуміння та боротьби з потенційними небезпеками. В залежності від джерела походження, загрози поділяють на екзогенні, що виникають зовні підприємства та зазвичай не залежать від його діяльності та ендогенні, які виникають всередині самого підприємства через його власну діяльність або недоліки у внутрішніх процесах (рис. 1).

Розглядаючи загрози за способом виникнення, можна розділити їх на активні і пасивні. Активні загрози включають в себе навмисне втручання атакуючих, наприклад, хакерські атаки, вірусні пошкодження, фішингові атаки тощо. Пасивні загрози, навпаки, виникають без безпосередньої участі зловмисників, наприклад, втрата даних через несправність обладнання, несанкціонований доступ через некомпетентність працівника тощо.

За способами протидії загрозам розрізняють превентивні заходи та реагувальні. Превентивні заходи, що спрямовані на запобігання виникненню загроз, наприклад, встановлення брандмауерів, оновлення програмного забезпечення. Реагувальні заходи, спрямовані на виявлення і ліквідацію вже існуючих загроз, наприклад, резервне копіювання даних, антивірусні системи тощо.

Особливу увагу слід звернути на типи шкоди, яку можуть завдати загрози, серед яких виділяють фінансові та репутаційні наслідки. Фінансові загрози призводять до фінансових втрат, наприклад, крадіжка даних для фінансових транзакцій, несанкціонований доступ до конфіденційної інформації тощо. Репутаційні ризики впливають на репутацію підприємства, такі як розголошення конфіденційної інформації, порушення законодавства з захисту даних тощо.

Для забезпечення інформаційної безпеки підприємства та сталого розвитку бізнесу, важливо виконати ряд завдань, серед яких – створення та впровадження комплексного плану інформаційної безпеки, розробка якого дозволить не тільки передбачити потенційні загрози, але й ефективно адаптуватися до них, враховуючи особливості діяльності і потреб компанії.

Структура та основні напрямки дій у рамках розробки комплексного плану забезпечення інформаційної безпеки підприємства наведено на рис. 4.

Крім того, цей план повинен передбачати регулярне оновлення заходів безпеки і включати в себе не тільки технічні аспекти, такі як захист від вірусів та шкідливого програмного забезпечення, але й організаційні заходи, такі як навчання персоналу основам кібергігієни та встановлення чітких правил реагування на інциденти.

Важливою складовою для підвищення ефективності плану є також розробка стратегії відновлення після настання можливих

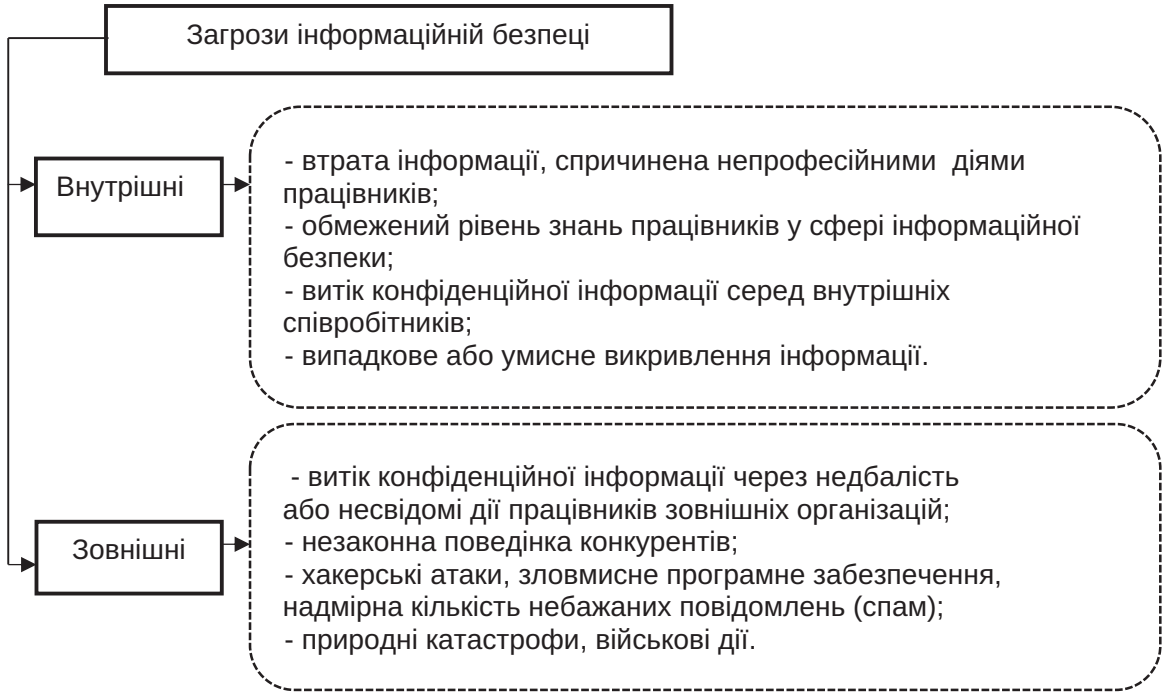

Рис. 3. Загрози інформаційній безпеці підприємства

Джерело: сформовано авторами на основі [5]

інцидентів, яка повинна включати в себе наступні практики:

1. Організація системного резервного копіювання важливих даних, зокрема конфіденційної інформації та облікових даних у надійні хмарні сховища;
2. Захист даних, що зберігаються в хмарі, шляхом їх шифрування для забезпечення конфіденційності;
3. Впровадження корпоративної електронної пошти для обміну інформацією та спільної роботи з документами, що забезпечує додатковий рівень захисту;
4. Розподіл прав доступу до важливих інформаційних ресурсів, в тому числі облікових даних між визначеними співробітниками;
5. Застосування двофакторної аутентифікації для надійного підтвердження особистості користувачів;
6. Використання сучасних комунікаційних платформ для забезпечення ефективної взаємодії між співробітниками під час дистанційної роботи;

Додатково, важливим аспектом забезпечення інформаційної безпеки підприємства. є посилення вимог до співробітників, особливо бухгалтерів, у сфері обробки інформації та використання сучасних технічних. Розробка та впровадження навчальних програм, спрямованих на підвищення обізнаності та навичок персоналу щодо коректного використання технологій та обробки конфіденційної інформації, може допомогти пристосувати співробітників до нових вимог та підтримати високий рівень їхньої кваліфікації. Це допоможе уникнути можливих ризиків безпеки, пов'язаних з недбалістю або неправильним використанням технічних засобів, а також збільшить загальний рівень захищеності інформації на підприємстві.

Висновки. В процесі дослідження встановлено, що забезпечення інформаційної безпеки є надзвичайно важливим аспектом для будь-якого підприємства. Проаналізовано різноманітні підходи до розуміння сутності поняття «інформаційна безпека» та визначено багатогранність даного поняття. Визначено, що інформаційна безпека не лише захищає конфіденційні дані підприємства, а й є важливою для забезпечення стійкої системи його економічної безпеки. Визначено фактори впливу та основні джерела загроз інформаційній безпеці підприємства. Сформовано комплексний план інформаційної безпеки, який дозволить передбачити можливі ризики та вжити необхідні заходи для їх попередження та мінімізації. Визначено, що ефективна реалізація цього плану потребує постійного моніторингу та адаптації до змін у сфері інформаційної безпеки.

Рис. 4. Комплексний план забезпечення інформаційної безпеки підприємства

Джерело: сформовано авторами на основі [2–6]

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» Закон України від 09.01.*2007* № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 18.04.2024)

2. Архипов О., Архипова Є. Особливості розуміння понять «інформаційна безпека» та «безпека інформації». Інформаційні технології та безпека: основи забезпечення інформаційної безпеки (ІТБ-2014): Матеріали XIV міжнародної науково-практичної конференції. Київ : ІПРІ НАН України, 2014. С. 18–30. URL: https://ktpu.kpi.ua/wp-content/uploads/2016/02/st-14_AA_Osoblivosti-rozuminnya-IB_BI.pdf (дата звернення: 14.04.2024)

3. Гнатенко, В. Інформаційно-економічна безпека як фактор стабільного розвитку держави. Публічне урядування. 2020. № 5 (25). С. 63–74. DOI: https://doi.org/10.32689/2617-2224-2020-5(25)-63-74 (дата звернення: 11.04.2024)

4. Захаров О. І. Інформаційне забезпечення управління системою економічної безпеки підприємства. URL: https://library.krok.edu.ua/media/library/category/statti/zakharov_0010.pdf (дата звернення: 10.04.2024)

5. Нехай В. А. Інформаційна безпека як складова економічної безпеки підприємств. *Науковий вісник Міжнародного гуманітарного університету. Серія : Економіка і менеджмент.* 2017. Вип. 24(2). С. 137–140. URL: http://nbuv.gov.ua/UJRN/Nvmgu_eim_2017_24%282%29__30 (дата звернення: 10.04.2024)

6. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського національного університету.* 2023. Серія ПРАВО. Випуск 78: частина 2. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/285994/280058 (дата звернення: 09.04.2024)

REFERENCES:

1. «Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 roky» Zakon Ukrainy vid 09.01.2007 № 537-V ["On the Basic Principles of Information Society Development in Ukraine for 2007–2015"]. Available at: https://zakon.rada.gov.ua/laws/show/537-16#Text (accessed April 18, 2024)

2. Arkhypov O., Arkhypova Ye. (2014) Osoblyvosti rozuminnia poniat «informatsiina bezpeka» ta «bezpeka informatsii» [Peculiarities of understanding the concepts "information security" and "information security"]. Informatsiini tekhnolohii ta bezpeka: osnovy zabezpechennia informatsiinoi bezpeky (ITB-2014): Materialy KhIV mizhnarodnoi naukovo-praktychnoi konferentsii. K.: IPRI NAN Ukrainy, pp. 18–30. Available at: https://ktpu.kpi.ua/wp-content/uploads/2016/02/st-14_AA_Osoblivosti-rozuminnya-IB_BI.pdf (accessed April 14, 2024)

3. Hnatenko, V. (2020) Informatsiino-ekonomichna bezpeka yak faktor stabilnoho rozvytku derzhavy. *Publichne uriaduvannia* [Information and economic security as a factor of stable development of the state], no. 5 (25), pp. 63–74. DOI: https://doi.org/10.32689/2617-2224-2020-5(25)-63-74 (accessed April 11, 2024)

4. Zakharov O. I. Informatsiine zabezpechennia upravlinnia systemoiu ekonomichnoi bezpeky pidpryiemstva [Information management of the economic security system of the enterprise]. Available at: https://library.krok.edu.ua/media/library/category/statti/zakharov_0010.pdf (accessed April 10, 2024)

5. Nekhai V. A. (2017) Informatsiina bezpeka yak skladova ekonomichnoi bezpeky pidpryiemstv [Information security as a component of economic security of enterprises]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu*. *Seriia: Ekonomika i menedzhment,* no. 24(2), pp. 137–140. Available at: http://nbuv.gov.ua/UJRN/Nvmgu_eim_2017_24%282%29__30 (accessed April 10, 2024)

6. Shevchuk M.O. (2023) Do pytannia henezy poniattia informatsiinoi bezpeky yak skladovoi natsionalnoi bezpeky [To the question of the genesis of the concept of information security as a component of national security]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia PRAVO.* Vol. 78. Available at: http://visnyk-pravo.uzhnu.edu.ua/article/view/285994/280058 (accessed April 9, 2024)