DOI: https://doi.org/10.32782/2524-0072/2024-70-147

УДК 354.332.12

ФОРМУВАННЯ СТРАТЕГІЇ ПОСИЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

DEVELOPMENT OF A STRATEGY FOR ENHANCING ENTERPRISE INFORMATION SECURITY

Мащенко Марина Анатоліївна
доктор економічних наук, професор,
Національний технічний університет «Харківський політехнічний університет»
ORCID: https://orcid.org/0000-0002-8863-6040

Іпполітов Євгеній Миколайович
здобувач PhD,
Національний технічний університет «Харківський політехнічний університет»
ORCID:https://orcid.org/0009-0001-3165-4141

Mashchenko Maryna, Ippolitov Yevhenii
National Technical University «Kharkiv Polytechnic Institute»

У статті розглянуті основні питання посилення інформаційної безпеки підприємства, визначено важливість її забезпечення для бізнесу в умовах стрімкого розвитку технологій. Проведено теоретичне дослідження підходів до визначення поняття «інформаційна безпека підприємства» різними науковцями. Були окреслені основні види інформаційної безпеки, які мають бути забезпечені під час функціонування підприємства. В процесі використання міжнародних стандартів у сфері інформаційних технологій було визначено необхідність дотримання законодавчих і нормативних вимог щодо захисту інформації. Запропоновано послідовність імплементації стандарту ISO/IEC 27001 на підприємстві, визначено можливі строки його впровадження та відповідальних. Визначено основні етапи формування стратегії посилення інформаційної безпеки підприємства. Це дозволить підприємству побудувати ефективну систему управління інформаційною безпекою, мінімізувати ризики інформаційних інцидентів.

Ключові слова: стратегія посилення інформаційної безпеки підприємства, інформаційна безпека підприємства, інформаційні ресурси підприємства, системи управління інформаційною безпекою, кіберзагрози.

The article considers the main issues of enhancing the information security of enterprise, determines the importance of its provision for business in the context of rapid development of technologies. The article conducts a theoretical study of approaches to definition of the concept of 'information security of an enterprise' by different scientists. The main functions performed by information security are defined. The main types of information security that should be ensured during the operation of an enterprise are considered. In the process of using international standards in the field of information technology, the need to comply with legislative and regulatory requirements for information security has been identified. The sequence of implementation of the ISO/IEC 27001 standard at an enterprise is proposed, possible terms of its implementation and those responsible are determined. The main stages of formation of a strategy for enhancing the information security of enterprise are defined. An effective strategy for enhancing information security should have clearly defined goals and objectives aimed at reducing risks, increasing the level of protection of information systems and ensuring compliance with modern standards. The purpose of implementing this strategy is to ensure reliable protection of confidential, critical and publicly available information from unauthorized access, leakage, loss or modification. Achieving this goal requires compliance with the following principles: ensuring confidentiality, maintaining integrity and guaranteeing accessibility. It is determined that the introduction of training and the formation of a culture of compliance with the principles of information security are important elements in the implementation of a strategy for enhancing information security. It is noted that the introduction of a strategy for enhancing the information security of an enterprise will allow the enterprise to build an effective information security management system, minimize the risks of information incidents, increase the level of trust from customers and partners, and ensure compliance with legislative and regulatory requirements. In further research, the authors will focus on developing enterprise information security management mechanisms to protect critical data.

Keywords: strategy for enhancing enterprise information security, enterprise information security, enterprise information resources, information security management systems, cyber threats.

Постановка проблеми. Сьогодні, в умовах стрімкого розвитку технологій і зростання кількості кіберзагроз, питання інформаційної безпеки підприємств набуває особливої важливості для бізнесу. Зі збільшенням обсягу цифрових даних на підприємствах зростає ризик кібератак і незаконного використання цієї інформації. Захист таких даних стає не просто необхідністю, а стратегічним пріоритетом. Для будь-якого підприємства, незалежно від сфери діяльності, актуальним залишається формування ефективної стратегії забезпечення інформаційної безпеки, що включає розробку та впровадження комплексу заходів для захисту конфіденційних даних та інформаційних процесів. Це передбачає також формування чітких вимог до персоналу, керівників і технічних служб. Важливо пам'ятати, що інформація стає одним із ключових активів бізнесу, і її втрата або пошкодження можуть спричинити значні фінансові збитки та підрив репутації. Тому забезпечення інформаційної безпеки підприємства включає не лише технічні рішення, але й організаційні заходи для захисту від подібних ризиків.

Аналіз останніх досліджень і публікацій. Значна кількість наукових досліджень присвячена проблематиці забезпечення інформаційної безпеки підприємства. Так, основні аспекти забезпечення та управління інформаційною безпекою підприємства розглянуто у працях таких науковців як: Носок С. О., Фаль О. М., Ткач В.М. [1], Рач В. А. [2]. Оцінюванню стану інформаційної безпеки підприємства приділено увагу Велігурою А. В. [3]. Ясінська А. розглядає інформаційну безпеку підприємства через призму формування засад ефективного захисту інформації [4]. Яремко С. М. та Кузьміна О. М. досліджували актуальні аспекти захисту інформаційних ресурсів саме в бізнес-структурах [5].

Виділення невирішених раніше частин загальної проблеми. Попри значний науковий доробок у сфері забезпечення інформаційної безпеки підприємства, залишаються питання, що потребують подальших досліджень та розвитку. Серед них – процес формування дієвої стратегії посилення інформаційної безпеки підприємства, а також її своєчасна імплементація задля виявлення і попередження потенційних загроз та мінімізація їх негативного впливу.

Формулювання цілей статті (постановка завдання). Метою статті є теоретичне обґрунтування процесу формування ефективної стратегії посилення інформаційної безпеки підприємства, яка враховуватиме сучасні виклики та специфіку інформаційного середовища.

Виклад основного матеріалу дослідження. Інформаційна безпека є одним із ключових аспектів діяльності сучасних підприємств, адже збереження конфіденційності, цілісності та доступності даних безпосередньо впливає на їхню конкурентоспроможність і стабільність. У світі, де цифровізація охопила практично всі сфери бізнесу, інформація стала стратегічним ресурсом, а її втрата або викрадення може завдати значних репутаційних і фінансових збитків для будь-якого підприємства.

Основними загрозами в інформаційній сфері підприємства є кіберзлочини, несанкціонований доступ до даних, внутрішні порушення безпеки та технічні збої. Ці проблеми виникають через швидке впровадження новітніх технологій без належної підготовки, недостатній рівень кіберграмотності персоналу, а також через збільшення кількості та складності кіберзагроз, які постійно еволюціонують.

В загальному розумінні, інформаційна безпека підприємства – це сукупність заходів, спрямованих на захист інформації від несанкціонованого доступу, розкриття, модифікації або знищення, з метою забезпечення її конфіденційності, цілісності та доступності. Крім того, можна погодитися з визначенням Велігури А. В., за яким, інформаційна безпека – «це комплекс заходів та засобів щодо забезпечення збереження інформації, що знаходиться в системі інформаційного забезпечення діяльності підприємства, переданої, оброблюваної, а також тієї, що зберігається та надається системою» [3]. За словами Тлумак О., інформаційна безпека – «це сукупність технологій, стандартів, політики та практик управління, які застосовуються до інформації для її збереження» [6]. В свою чергу, під інформаційною безпекою підприємства Верескун М. В. розуміє «сукупність усіх елементів системи управління, зокрема і стратегічного, які пов'язані з визначенням, формуванням конфіденційності, цілісністю та доступністю, відповідною підзвітністю, автентичністю та достовірністю інформації або засобів її обробки на підприємстві» [7, с. 55].

Важливість забезпечення інформаційної безпеки не викликає сумнівів, тому необхідно визначити, які ж функції для підприємства вона виконує. Серед основних функцій такі: забезпечення безпечної роботи програмного забезпечення, реалізованої в системах інфор-

маційних технологій будь-якого підприємства; здійснення захисту даних, які підприємство збирає та використовує; захист технологічних активів, що використовуються на підприємстві; захист спроможності підприємства функціонувати.

Розрізняють такі основні види інформаційної безпеки підприємства: технічна, організаційна, фізична, криптографічна та правова. Технічна інформаційна безпека виявляється через захист технічних засобів і систем, таких як сервери, мережеві пристрої, робочі станції та програмне забезпечення. Крім того, шляхом використання антивірусних програм, міжмережевих екранів (фаєрволів), систем виявлення та запобігання вторгненням (IDS/IPS). Організаційна інформаційна безпека забезпечує впровадження політик, процедур та регламентів, які регулюють доступ до інформації та її використання, а також вимагає додержання контролю виконання правил безпеки співробітниками. Наступним проявом інформаційної безпеки є фізична інформаційна безпека, яка забезпечує захист фізичних об'єктів, де зберігається чи обробляється інформація (серверні кімнати, архіви, офісні приміщення) та передбачає застосування засобів відеоспостереження, контролю доступу, охоронних сигналізацій. В умовах цифровізації особливого значення набуває криптографічна інформаційна безпека, яка проявляється через захист інформації шляхом її шифрування, щоб запобігти несанкціонованому доступу чи викраденню. Також вона враховує використання цифрових сертифікатів, електронного підпису та інших технологій шифрування. І останнім видом інформаційної безпеки виступає правова інформаційна безпека, яка вимагає дотримання законодавчих і нормативних вимог щодо захисту інформації, таких як регламенти GDPR, ISO 27001 та інші, а також оформлення договірних зобов'язань щодо конфіденційності з партнерами, співробітниками та клієнтами.

Використання міжнародних стандартів у сфері інформаційної безпеки є важливим інструментом для підвищення рівня захисту інформаційних ресурсів підприємства. Ці стандарти надають уніфіковані підходи, які допомагають організаціям створювати та впроваджувати ефективні системи управління інформаційною безпекою (СУІБ).

Одним із найвідоміших і широко використовуваних стандартів є ISO/IEC 27001 [8]. Він визначає вимоги до побудови, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою. Основна мета стандарту – забезпечити конфіденційність, цілісність і доступність інформації, а також знизити ризики, пов'язані з її обробкою. Процес імплементації стандарту ISO/IEC 27001 на підприємстві наведено на рис. 1. та деталізовано у табл. 1.

Процес використання міжнародних стандартів починається з оцінки відповідності поточного стану захисту інформації підприємства вимогам стандартів. Це включає аналіз існуючих політик, процедур і технічних засобів, а також виявлення прогалин. Далі організація визначає основні ризики, які можуть вплинути на безпеку інформаційних активів, і розробляє план їхньої мінімізації. Стандарт ISO/IEC 27001, наприклад, передбачає проведення ризик-менеджменту, що включає ідентифікацію загроз, оцінку їхнього впливу та ймовірності, а також впровадження захо-

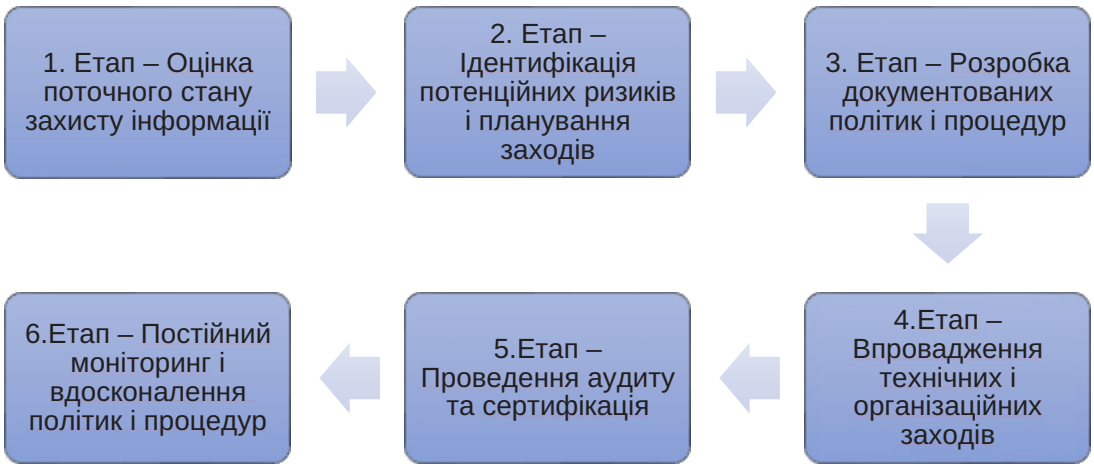

Рис. 1. Процес імплементації стандарту ISO/IEC 27001

Джерело: розроблено авторами

Таблиця 1

Послідовність запровадження стандарту ISO/IEC 27001 на підприємстві

Назва етапу та послідовність	Сутність	Орієнтовні строки впровадження	Відповідальні
1. Оцінка поточного стану	Аналіз існуючих політик, процедур і технічних засобів. Виявлення прогалин у відповідності вимогам стандарту.	1-2 місяці	Відділ інформаційної безпеки, керівництво
2. Ідентифікація ризиків і планування заходів	Визначення основних ризиків для інформаційних активів. Проведення ризик-менеджменту, оцінка загроз і розробка плану мінімізації ризиків.	2-3 місяці	Відділ інформаційної безпеки, аналітики, керівництво
3. Розробка документованих політик і процедур	Створення політик доступу, управління інцидентами, резервного копіювання та планів дій на випадок надзвичайних ситуацій.	1-2 місяці	Відділ інформаційної безпеки, юридичний відділ, керівництво
4. Впровадження технічних і організаційних заходів	Установлення систем шифрування, моніторингу, контролю доступу та засобів виявлення загроз.	3-4 місяці	IT-відділ, відділ інформаційної безпеки, персонал
5. Проведення аудиту та сертифікація	Перевірка відповідності процесів і заходів вимогам стандарту. Проведення сертифікації для отримання офіційного підтвердження.	1-2 місяці	Зовнішні аудитори, відділ інформаційної безпеки, керівництво
6. Постійний моніторинг і вдосконалення	Регулярний перегляд заходів безпеки, оновлення політик і технічних рішень відповідно до змін у загрозах і технологіях.	Постійно	Відділ інформаційної безпеки, персонал, керівництво

Джерело: розроблено авторами

дів контролю для їх усунення або зниження. Важливим етапом є розробка документованих політик і процедур відповідно до вимог стандарту. Це можуть бути політики доступу до інформації, управління інцидентами, резервного копіювання, а також плани дій на випадок непередбачуваних ситуацій. Наступний крок – впровадження технічних і організаційних заходів, визначених стандартами. Це може включати встановлення систем шифрування даних, налаштування засобів контролю доступу, впровадження систем моніторингу та виявлення загроз. Після впровадження стандартів підприємство має пройти аудит для перевірки відповідності своїх процесів вимогам стандарту. У разі успішного проходження сертифікації організація отримує офіційне підтвердження відповідності, що підвищує її репутацію та довіру клієнтів і партнерів. Постійний моніторинг і вдосконалення є завершальним, але безперервним етапом. Інформаційні загрози еволюціонують, тому стандарти передбачають регулярний перегляд і оновлення заходів безпеки.

Таким чином, використання міжнародних стандартів дозволяє підприємствам побудувати системний підхід до захисту інформації, підвищити ефективність управління ризиками та забезпечити відповідність сучасним вимогам і очікуванням ринку.

В свою чергу, формування стратегії посилення інформаційної безпеки є ключовим кроком у забезпеченні захисту інформаційних активів підприємства. Ця стратегія повинна мати чітко визначені цілі та завдання, які спрямовані на зменшення ризиків, підвищення рівня захисту інформаційних систем і забезпечення відповідності сучасним стандартам.

Основна мета формування стратегії посилення інформаційної безпеки підприємства – забезпечити надійний захист конфіденційної, критичної та загальнодоступної інформації

від несанкціонованого доступу, витоку, втрати чи модифікації. Досягнення цієї мети потрібно передбачити виконання наступних принципів:

– забезпечення конфіденційності – гарантування доступу до інформації лише для уповноважених осіб;

– підтримання цілісності – запобігання зміні чи пошкодженню інформації;

– гарантування доступності – забезпечення доступу до інформації в потрібний час і в необхідному обсязі.

Враховуючи основні вимоги міжнародних стандартів забезпечення інформаційної безпеки було запропоновано наступну послідовність формування стратегії посилення інформаційної безпеки підприємства, яка буде складатись з таких основних етапів:

1. Аналіз вимог існуючих міжнародних стандартів та впливів зовнішнього середовища на забезпечення інформаційну безпеки.

2. Оцінювання ризиків і вразливостей шляхом проведення аналізу поточного стану забезпечення інформаційної безпеки, ідентифікація основних загроз й слабких місць у системах і процесах підприємства та стану технічної архітектури на підприємстві.

3. Аналіз отриманих результатів та визначення напрямів для удосконалення.

4. Формування системи стратегічних цілей посилення інформаційної безпеки підприємства.

5. Запровадження заходів, спрямованих на імплементацію запропонованої стратегії, а саме:

– запровадження політики безпеки через розроблення чітких і зрозумілих правил, які регулюють доступ до інформаційних ресурсів, обробку та зберігання даних;

– здійснення технічного посилення захисту шляхом встановлення систем шифрування, антивірусного програмного забезпечення, засобів контролю доступу та моніторингу;

– підвищення обізнаності персоналу через проведення навчальних заходів для співробітників з метою ознайомлення їх із ризиками, правилами безпеки та кроками, яких необхідно дотримуватися для запобігання інцидентам;

– запровадження інцидент-менеджменту шляхом створення процедур реагування на інформаційні інциденти, включаючи виявлення, аналіз, усунення наслідків та впровадження запобіжних заходів;

– відстеження на відповідність стандартам через орієнтацію на міжнародні стандарти інформаційної безпеки для забезпечення системності та ефективності впроваджених заходів.

6. Затвердження розробленої стратегії, імплементація на підприємстві та перевірка її виконання.

7. Контролювання процесу реалізації стратегії та її коригування в разі необхідності.

8. Здійснення безперервного моніторингу і вдосконалення шляхом створення системи постійного аналізу стану інформаційної безпеки та оновлення заходів захисту відповідно до змін у технологіях і потенційних загрозах.

Таким чином, запровадження стратегії посилення інформаційної безпеки підприємства дозволить підприємству побудувати ефективну систему управління інформаційною безпекою, мінімізувати ризики інформаційних інцидентів, підвищити рівень довіри з боку клієнтів і партнерів, а також забезпечити відповідність законодавчим і регуляторним вимогам.

Одним із ключових аспектів ефективної реалізації стратегії інформаційної безпеки є залучення персоналу. Навчання співробітників і формування культури безпеки забезпечують їхню обізнаність, підвищують відповідальність за дотримання процедур і мінімізують ризики людських помилок, які залишаються однією з головних причин інцидентів у сфері інформаційної безпеки.

Головною метою навчання персоналу під час запровадження стратегії посилення інформаційної безпеки є забезпечення співробітників знаннями та навичками, необхідними для виконання їхніх обов'язків у межах політик інформаційної безпеки. Це повинно враховувати:

– розуміння основ інформаційної безпеки;

– наявність навичок розпізнавання загроз, таких як фішингові атаки, шкідливе програмне забезпечення тощо;

– знання процедур реагування на інциденти безпеки.

В процесі навчання персоналу можна надати перевагу таким формам навчання як: тренінги та семінари, які проводяться спеціалістами з інформаційної безпеки або зовнішніми експертами; онлайн-навчання – забезпечує зручний формат навчання для співробітників, особливо у великих або розподілених компаніях; практичні вправи, включають в себе симуляції кіберзагроз, які дозволяють персоналу перевірити свої знання в реальних сценаріях; інструкції та пам'ятки шляхом розповсюдження матеріалів з основними правилами та процедурами.

Особливо важливо проводити базові тренінги для нових співробітників під час адаптації та організовувати регулярні оновлення знань для всього персоналу, особливо у відповідь на нові загрози або оновлення політик. Крім того, формування культури інформаційної безпеки персоналу підприємства стає критично необхідною процедурою. Керівництво має демонструвати відповідальне ставлення до дотримання політик інформаційної безпеки, здійснювати операційну діяльність відповідно до встановлених процедур, Отже, впровадження навчання та формування культури дотримання принципів інформаційної безпеки є важливими елементами під час імплементації стратегії посилення інформаційної безпеки, що дозволяють не тільки знизити ризики, але й підвищити загальну стійкість підприємства до сучасних внутрішніх та зовнішніх загроз.

Висновки. Отже, потреба у формуванні дієвої стратегії посилення інформаційної безпеки підприємства зумовлена стрімким зростанням обсягу даних, що використовуються у бізнес-процесах та розвитком цифрових технологій. Однак це також підвищує ризики витоку чи неправомірного використання даних. Основні загрози стосуються інформації, що зберігається в інформаційних системах підприємства, таких як програмне забезпечення, текстові редактори та бази даних. Саме тому, необхідно надавати доступ лише ідентифікованим та верифікованим користувачам із чітко визначеними повноваженнями. Формування стратегії інформаційної безпеки є важливим етапом у забезпеченні захисту даних. Вона повинна включати комплексну оцінку ризиків, визначення пріоритетів захисту та впровадження технічних і організаційних заходів для мінімізації загроз. Ефективність стратегії посилення інформаційної безпеки залежить від точності виявлення, аналізу та оцінки ризиків, що є критичним етапом у процесі її розробки. У подальших дослідженнях автори зосередять увагу на розробленні механізмів управління інформаційною безпекою підприємства для захисту критичних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Управління інформаційною безпекою: конспект лекцій : навч. посіб. для студ. спец. 125 «Кібербезпека». Уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.

2. Рач В. А. Проблеми захисту інформації в управлінні проектами в епоху економіки знань. *Управління проектами та розвиток виробництва: зб.наук.пр.* Луганськ: вид-во СНУ ім. В. Даля. 2009. № 2 (30). С. 156-160. URL: http://www.pmdp.org.ua/images/Journal/30/09rvaeez.pdf (дата звернення: 30.12.2024).

3. Велігура А. В. Оцінювання стану інформаційної безпеки підприємства. Управління проектами та розвиток виробництва. 2014. № 4(52). С. 28–39.

4. Ясінська А. Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації. *Економіка та суспільство.* 2023. URL: https://doi.org/10.32782/2524-0072/2023-56-118 (дата звернення: 30.12.2024).

5. Яремко С.М, Кузьміна О. М. Актуальні аспекти захисту інформаційних ресурсів бізнес-структур. *Вісник Хмельницького національного університету.* 2020. № 5 С. 238–242.

6. Тлумак О. Інформаційна безпека підприємства: сучасні виклики та загрози. URL: https://ena.lpnu.ua:8443/server/api/core/bitstreams/7cbea921-7393-42a4-91d4-364acc52e304/content (дата звернення: 30.12.2024).

7. Верескун М. В. Методичне забезпечення системи інформаційної безпеки промислових підприємств. *Економіка і організація управління*. 2014. Вип. 1–2. С. 54–60.

8. Основні переваги сертифікації ISO/IEC 27001. URL https://www.issp.training/post/osnovni-perevahy-sertyfikatsiyi-iso-iec-27001(дата звернення: 30.12.2024).

REFERENCES:

1. Nosok S. O., Fal O. M., Tkach V. M. (2021) Upravlinnia informatsiinoiu bezpekoiu: konspekt lektsii : navch. posib. dlia stud. spets. 125 «Kiberbezpeka» [Information Security Management: A Textbook for Students of Specialty 125 "Cybersecurity"]. Kyiv : KPI im. Ihoria Sikorskoho, 258 p. (in Ukrainian)

2. Rach V. A. (2009) Problemy zakhystu informatsii v upravlinni proektamy v epokhu ekonomiky znan [Problems of Information Protection in Project Management in the Era of the Knowledge Economy]. *Upravlinnia proektamy ta rozvytok vyrobnytstva – Project management and production development*, vol. 2(30), pp. 156–160. Available at: http://www.pmdp.org.ua/images/Journal/30/09rvaeez.pdf (accessed Desember 30, 2024)

3. Velihura A. V. (2014) Otsiniuvannia stanu informatsiinoi bezpeky pidpryiemstva [Assessment of the state of information security of the enterprise]. *Upravlinnia proektamy ta rozvytok vyrobnytstva – Project management and production development*, vol. 4(52), pp. 28–39.

4. Yasinska A. (2023) Informatsiina bezpeka pidpryiemstva: kontseptualni zasady efektyvnoho zakhystu informatsii [Enterprise Information Security: Conceptual Principles of Effective Information Protection.]. *Ekonomika ta suspilstvo – Economy and Society*, DOI: 10.32782/2524-0072/2023-56-118.

5. Yaremko S. M, Kuzmina O. M. (2020) Aktualni aspekty zakhystu informatsiinykh resursiv biznes-struktur [Current aspects of protecting information resources of business structures]. Visnyk Khmelnytskoho natsionalnoho universytetu – *Bulletin of Khmelnytskyi National University*, vol. 5, pp. 238–242.

6. Tlumak O. Informatsiina bezpeka pidpryiemstva: suchasni vyklyky ta zahrozy [Enterprise information security: modern challenges and threats]. Available at: https://ena.lpnu.ua:8443/server/api/core/bitstreams/7cbea921-7393-42a4-91d4-364acc52e304/content (accessed Desember 30, 2024).

7. Vereskun M. V. (2014) Metodychne zabezpechennia systemy informatsiinoi bezpeky promyslovykh pidpryiemstv [Methodological support of the information security system of industrial enterprises]. *Ekonomika i orhanizatsiia upravlinnia – Economics and management organization*, vol. 1–2, pp. 54–60.

8. Osnovni perevahy sertyfikatsii ISO/IEC 27001 [Key benefits of ISO/IEC 27001 certification]. Available at: https://www.issp.training/post/osnovni-perevahy-sertyfikatsiyi-iso-iec-27001 (accessed Desember 30, 2024).