DOI: https://doi.org/10.32782/2524-0072/2023-56-118

УДК 338:004.7.056

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА: КОНЦЕПТУАЛЬНІ ЗАСАДИ ЕФЕКТИВНОГО ЗАХИСТУ ІНФОРМАЦІЇ

INFORMATION SECURITY OF THE ENTERPRISE: CONCEPTUAL FRAMEWORK FOR EFFECTIVE INFORMATION PROTECTION

Ясінська Алла Іванівна
кандидат економічних наук, доцент,
Національний університет «Львівська політехніка»
ORCID: http://orcid.org/0000-0002-5445-8987

Yasinska Alla
Lviv Politechnic National University

У статті розкрито проблематику щодо захисту інформації в системі управління підприємством. Обґрунтовано необхідність та доцільність застосування процедури інформаційної безпеки задля належного захисту та збереження її цілісності, корисності та актуальності. Досліджено сутність поняття комерційної таємниці та конфіденційної інформації на законодавчому рівнях. Визначено основні складові моделі інформаційної безпеки, зокрема джерела загроз (зовнішні та внутрішні), об'єкти загроз, а також у складі захисту інформації розподіл її за категоріями (публічна та з обмеженим доступом). Наведено характеристику видів захисту інформації на документальному та технічному рівнях. Досліджено різновиди методів та інструментів задля підвищення захисту, які доцільно застосовувати, їх взаємозв'язок з інформаційними джерелами та розпорядниками інформації.

Ключові слова: конфіденційна інформація, комерційна таємниця, інформаційна безпека, захист облікових даних, модель інформаційної безпеки.

The article discloses the issue of information protection in the enterprise management system. The development of digital technologies, which contributes to the efficiency of creating, receiving and transmitting information, in the process of using electronic document flow, information networks, forming a database, using online transactions, storing data in cloud storage, etc., greatly complicates the process of protecting information, and therefore arises the need to implement appropriate information security measures. In the course of the study, the concepts of commercial secrets and confidential information at the legislative level were considered, problematic aspects were identified regarding regulatory and legal support and regulation of relations in the field of confidential information, its proper protection and actions in case of violation of the legal regime. The necessity and expediency of applying the information security procedure for the proper protection and preservation of its integrity, usefulness and relevance are substantiated. The main components of the information security model are identified, in particular, sources of threats and their possible threatening impact (external and internal), objects of threats (data, databases, information), as well as the division of information into categories (public and restricted) as part of information protection. The author characterizes the types of information protection at the documentary and technical levels, summarizes the measures and actions required to implement an appropriate protection system. Various methods and tools for improving the information security system, their relationship with information sources and information managers (owners) are investigated. Implementing a reliable information security system and protecting credentials should be a priority in the effective management of an enterprise; monitoring and analyzing the emergence of new threats, preventing them and finding ways to minimize them requires constant improvement and research, but will help to preserve important information.

Keywords: confidential information, trade secret, information security, credential protection, information security model.

Постановка проблеми. Динамічний розвиток технологічних інновацій, впровадження цифрових технологій, які застосовуються для побудови інформаційної системи управління підприємством значною мірою ускладнюють процес захисту інформації. Тому сьогодні

одним із головних завдань цифрового світу є захист інформації, збереження її цілісності та конфіденційності. Конфіденційна інформація за рівнем важливості потребує найвищого рівня безпеки і захищеності, для запобігання несанкціонованому доступу хакерів або шкідливих програм. Як правило, саме такі дані повинні бути захищені та недоступні стороннім особам. На законодавчо-нормативному рівні існують певні стандарти кібербезпеки та захисту даних, які встановлені, наприклад, в США – Федеральною торговою комісією (FTC), у Європі – Загальним регламентом захисту даних (GDPR), в Австралії – Австралійським центром кібербезпеки (ACSC).

На сьогоднішній день в Україні на законодавчо-нормативному рівні недостатньо врегульовані питання щодо захисту інформації, збереження її конфіденційності, і тому виникає потреба у забезпеченні цього захисту самим підприємством. Враховуючи значну кількість загроз, які можуть призвести до витоку конфіденційної інформації проблема її захисту є надзвичайно актуальною. Інформаційна безпека є складним процесом, який повинен включати в себе різноманітні заходи та дії, і доцільним є застосування системно-комплексного підходу з точки зору організаційних, технічних і правових заходів. Інформаційна безпека підприємства повинна включати в себе насамперед концептуальні засади щодо ефективного захисту інформації.

Аналіз останніх досліджень і публікацій показує, що питанням захисту інформації, зокрема облікової присвячені дослідження Легенчука С. Ф., Назаренка Т. П., Царук І. М. [1], Шишкової Н. Л. [2], Ахрамовича В. М., Амелькіна С. В. [3], Варічевої Р. В. [4], Осмятченко В. О., Склярук І. П. [5], Скрипника С. В., Франчук І. Б., Шепель І. В. [6] та інших. Одностайно всі науковці схиляються до думки і стверджують, що в сучасному інформаційному середовищі вже неможливо забезпечити успішне функціонування підприємств без управління процесами інформаційної безпеки.

Формулювання цілей статті (постановка завдання). Метою і завданням статті є формулювання концептуальних засад щодо побудови ефективної моделі інформаційної безпеки підприємства.

Виклад основного матеріалу дослідження. Розвиток інформатизації та активне впровадження цифрових технологій на підприємствах пов'язані не тільки з масштабами бізнесу, але й з складними умовами функціонування вітчизняних підприємств. Інформаційні технології здійснюють значний вплив на побудову системи управління підприємством, і задля ефективного функціонування особливу увагу слід звернути на концептуальні основи щодо захисту облікової інформації. Облікова інформація сформована в системі бухгалтерського обліку в процесі обробки, перетворення та інтерпретації є корисною для багатьох зацікавлених користувачів (зовнішніх, внутрішніх), є основою для прийняття управлінських рішень в системі управлінського обліку, тому ключовим питанням від якого залежатиме якість цієї інформації є насамперед її цілісність, захист та безпека.

Інформація, яка слугує для прийняття управлінських рішень, сформована в системі управлінського обліку є комерційною таємницею підприємства, містить конфіденційні дані, тому актуальним питанням є захист цієї інформації в системі фінансової безпеки кожного підприємства.

Правовий режим конфіденційної інформації в Україні регулюється Законом України «Про інформацію» [9]. У статті 21 цього Закону зазначено, що конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежений фізичною або юридичною особою, крім суб'єктів владних повноважень.

Також, визначення комерційної таємниці міститься в Цивільному та Господарському Кодексах України [12; 13]. Зокрема, це інформація, яка є секретною в тому розумінні, що вона загалом чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які зазвичай мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних наявним обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Варто зазначити, що конкретного переліку інформації, яка може бути конфіденційною чи комерційною таємницею, чинне законодавство України не визначає. Натомість ч. 4 ст. 21 Закону України «Про інформацію» [9] містить перелік відомостей, доступ до яких не може бути обмежений (зокрема, це інформація про стан довкілля, якість харчових продуктів, аварії, катастрофи та надзвичайні ситуації, стан здоров'я населення). Постанова КМУ «Про перелік відомостей, ще не становлять комерційної таємниці» № 611 від 09.08.1993 р. [11] визначає перелік відомостей,

що не можуть бути віднесені до комерційної таємниці (зокрема, відомості про чисельність і склад працівників, розмір заробітної плати, наявність вільних робочих місць, документи про сплату податків та обов'язкових платежів).

Таким чином, виходячи з наведених положень діючих законодавчо-нормативних актів, можна зробити висновок, що поняття «конфіденційна інформація» є ширшим ніж поняття «комерційна таємниця», тому комерційна таємниця є конфіденційною інформацією. Відомості та інформація, яка повинна бути обмежена у доступі керівництво має право визначати самостійно, як правило, до таких відносять: організаційного, технічного, комерційного, виробничого, технологічного та іншого характеру, і зазвичай, це інформація про собівартість продукції (робіт, послуг), методи та технології, дані про клієнтів, стратегію розвитку, маркетингові плани, умови договорів, розроблені проєкти, зразки, ноу-хау тощо. Але, задля захисту інформації і з метою збереження її конфіденційності та неправомірного використання доцільним є аналізування в першу чергу джерел загроз та визначення наслідків від їхнього впливу, тому для глибшого розуміння даного процесу варто системно впроваджувати певні заходи щодо інформаційної безпеки шляхом реалізації концептуальної моделі (рис. 1).

Концептуальна модель інформаційної безпеки підприємства дає змогу послідовно реалізувати основну її мету – впровадити належний захист інформації, зберегти її цілісність, актуальність та корисність, унеможливити протиправні дії з інформацією тощо.

Основними складовими концептуальної моделі інформаційної безпеки підприємства є визначення загроз: джерела (зовнішні та внутрішні), об'єкти загроз та їхня мета. Наступна складова – це захист інформації, який передбачає її розподіл за категоріями: відкрита та з обмеженим доступом, а також використання методів та інструментів задля підвищення захисту, і взаємозв'язок з джерелами та розпорядниками інформації.

Варто зазначити, що важливим аспектом в реалізації безпекових заходів є розподіл інформації за категоріями: відкрита та з обмеженим доступом, характеристику яких узагальнено у (табл. 1). Розподіл інформації за категоріями визначає її важливість і цінність для підприємства, і здійснювати цей розподіл потрібно враховуючи специфіку діяльності, масштаби, особливості технологічного, організаційного та виробничого характеру, фінансову політику та інші чинники.

Щодо видів захисту інформації доцільним є виокремлення за двома напрямками: документальний та технічний. Документальний передбачає розробляння корпоративних положень та інструкцій, а технічний – реалізацію певних заходів та дій, характеристику яких узагальнено у (табл. 2).

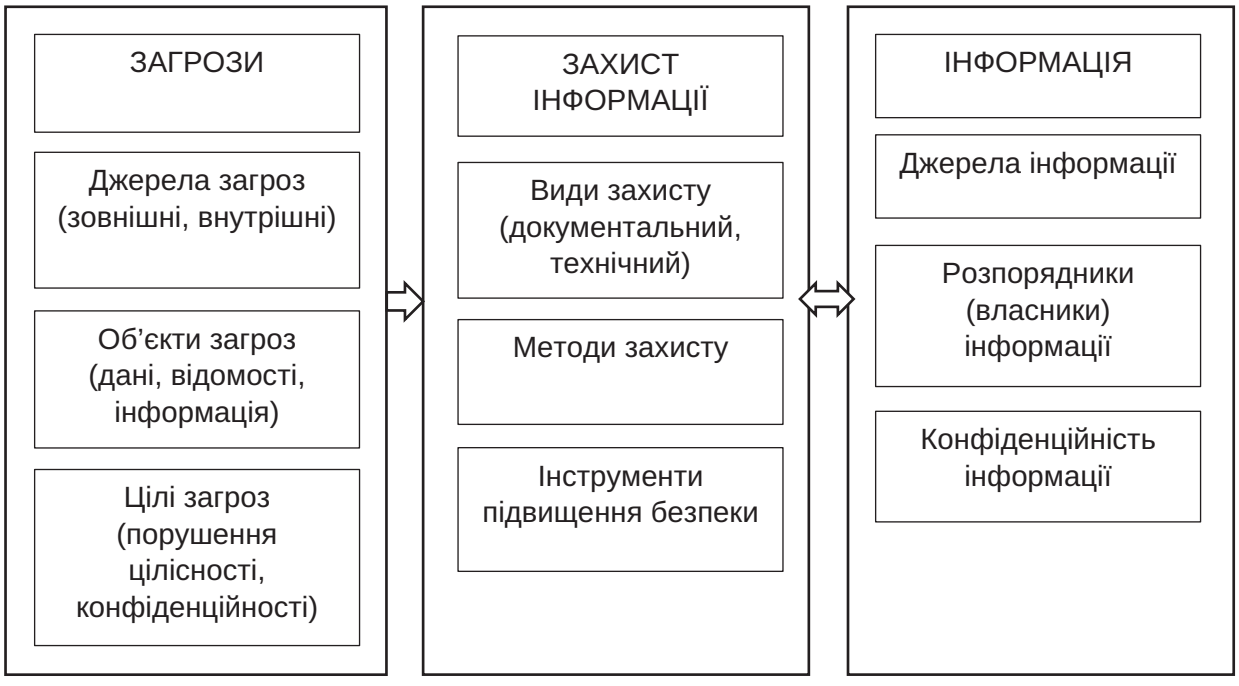

Рис. 1. Концептуальна модель інформаційної безпеки підприємства

Джерело: розроблено автором на основі [1–7]

Таблиця 1

Категорії розподілу інформації

Категорії		Характеристика
Відкрита	Публічна	інформація, яка була створена, задокументована, відображена на будь-яких носіях в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством; є відкритою та доступною для зацікавлених осіб (фізичних, юридичних, інших об'єднань, органів державної влади тощо) згідно Закону України «Про доступ до публічної інформації»
В обмеженим доступом	Службова	внутрішня інформація, яку підприємство – розпорядник інформації – не вважає за потрібне розголошувати. Наприклад, зміст доповідних записок або проекти і пропозиції, які виникають під час підготовки управлінських рішень
	Таємна	інформація, розголошення якої може зашкодити людині, суспільству чи державі. Наприклад, координати військових баз. Таємниця буває державна, комерційна, професійна, військова, банківська, адвокатська, лікарська, а також таємниця голосування, страхування, усиновлення нотаріальних дій тощо
	Конфіденційна	інформація, яку людина чи юридична особа (крім державних органів чи установ) не хоче розголошувати або є встановлює свої умови для розголошення. В процесі взаємодії між суб'єктами правовідносин відбувається обмін певними відомостями: роботодавців та найманих працівників, підрядників і замовників, партнерів та інших осіб. Якщо така інформація, має цінність для її власника, то він, відповідно докладатиме зусиль для правового захисту від нецільового використання та розголошення

Джерело: узагальнено на основі [3; 4; 8; 9; 10]

Таблиця 2

Види захисту інформації

Види захисту	Характеристика заходів та дій
Документальний	Розробляння корпоративних положень та інструкцій: – складання і підписання угоди про нерозголошення конфіденційної інформації (NDA) з кожним із співробітників, клієнтів, інвесторів, постачальників, підрядників, контрагентів, стажерів тощо; – розробляння Положення про захист конфіденційності: письмове зобов'язання працівників про не порушення норм Положення; – розробляння внутрішніх процедур щодо поводження з конфіденційною інформацією: порядок, правила доступу; пересилання; доступ третіх осіб; перелік співробітників, яким дозволено доступ до тієї чи іншої інформації; алгоритм дії у випадку порушення захисту конфіденційної інформації тощо;
Технічний	Реалізація технічних заходів та дій: – визначення переліку осіб, які матимуть доступ до конфіденційної інформації на певний період часу тобто в яких масштабах є потреба у впровадженні захисних алгоритмів, і в яких місцях ці алгоритми є уразливими; – постійний моніторинг та контроль за використанням конфіденційної інформації користувачами: пересилання, заміна, доповнення, видаляння, перегляд тощо; – розробляння правил внутрішньої (корпоративної) системи для роботи і спілкування співробітників: таск-менеджер, чат-системи, уникаючи спілкування через відкриті джерела (наприклад, Телеграм, Facebook тощо); – встановлення паролів: криптографічне шифрування ПК, паролі доступу до папок з конфіденційною інформацією, особисті паролі доступу в корпоративну систему для кожного співробітника; – встановлення системи захисту від кібератак: превентивні засоби захисту, процедуру резервного копіювання конфіденційної інформації, визначений алгоритм дії в разі кібератак або іншого порушення захисту конфіденційної інформації тощо.

Джерело: узагальнено на основі [1; 3; 4]

Розвиток цифрових технологій з одного боку сприяє оперативності створення, отримання та передачі інформації, а з іншого – електронний документообіг, мережево-комп'ютерна форма обліку, формування і використання бази даних, онлайн-транзакції, зберігання даних у хмарних сховищах значною мірою ускладнюють процес захисту, тому виникає потреба у використанні надійних методів захисту інформації, основними з яких можна виокремити наступні (табл. 3).

Інструменти задля підвищення інформаційної безпеки сприятимуть виявленню недоліків в інформаційній системі підприємства, захищатимуть дані, підтримуватимуть її функціональність та забезпечать певний рівень безпеки. Основними з них можуть бути:

– програмне забезпечення для захисту від вірусів та шкідливих програм;
– захист від витоку даних (DLP);
– система виявлення вторгнень (IDS) та запобігання вторгненням (IPS);
– брандмауери;
– віртуальні приватні мережі (VPN);
– сегментація мережі;
– інструменти видалення даних тощо.

Таким чином, узагальнюючи вище викладене можна сказати, що одним з головних завдань в цифровому середовищі є захист та безпека інформації. Для запобігання кібератак, уникнення витоку чи втрати даних, руйнівного впливу різного виду загроз, насанкціонованому доступу хакерів, вірусів, шкідливих програм тощо, необхідним є побу-

Таблиця 3

Методи захисту інформації

Методи захисту	Сутність методів
Класифікація та організація даних	процес організації даних за певними категоріями, які спрощують доступ, ранжування даних за критичністю для зменшення витрат на зберігання та резервне копіювання. Організація даних дозволяє визначити рівень ризику даних (низький, середній, високий), визначити загальнодоступну та приватну інформацію та застосувати відповідні для кожного рівня конфіденційності заходи безпеки. Політика класифікації дозволяє здійснити оцінку використання конфіденційності даних, забезпечити кращу конфіденційність та захист даних
Шифрування даних	метод полягає в кодуванні даних криптографами з використанням складних алгоритмів і шифрів для захисту даних від крадіжки або розкриття. У разі крадіжки зашифрованих даних їх майже неможливо розшифрувати без ключа дешифрування. Шифрування даних забезпечує конфіденційність під час передачі інформації та дозволяє виконувати процеси аутентифікації. Компаніям, які працюють із особливо конфіденційними даними, слід використовувати саме метод шифрування
Оцінка на захист персональних даних (DPIA)	оперативні інструменти для захисту корпоративної інформації, пов'язаної з високим ризиком розкриття особистої інформації. У рамках DPIA організації повинні: визначити характер, обсяг, контекст та мету обробки даних; оцінити ризики; визначити заходи для кожного ризику; забезпечити відповідність безпековим вимогам
Маскування (обфускація) даних	один із способів даних за допомогою заміни оригінальних даних на фіктивні. Маскування даних також використовується всередині компанії, щоб приховати інформацію від розробників, випробувачів та інших фахівців
Багатофакторна автентифікація	використання пароля та аутентифікація є одним з найпростіших методів забезпечення безпеки. Дані великих корпорацій досить часто перебувають у даркнеті. Корпоративні користувачі можуть використовувати багатофакторну автентифікацію та тим самим захистити конфіденційну інформацію
Резервні копії	основою всіх рішень безпеки є управління даними та резервне копіювання. Резервне копіювання слід виконувати щонайменше 1 раз на тиждень
Надійна мережева безпека	передбачається використання безлічі рішень безпеки для кращого захисту конфіденційних даних від крадіжки та несанкціонованого доступу

Джерело: узагальнено на основі [3; 4]

дова ефективної та дієвої системи захисту з використанням потужних методів кібербезпеки.

Висновки. Динамічний розвиток цифрових технологій в умовах сьогодення та активна діджиталізація бізнес-процесів підприємств здійснюють значний вплив на формування інформаційного середовища. На сьогоднішній день, інформацію вважають однією зі складових активів бізнесу, а полювання за нею стає одним із нових видів діяльності. Впроваджувати системи захисту інформації чи ні – це вибір кожного, але для того, щоб бізнес був у безпеці, і були збережені унікальність та конкурентоспроможність необхідно все ж таки, вжити заходи безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Легенчук С. Ф., Назаренко Т. П., Царук І. М. Принципи захисту даних у системі обліку: управлінські аспекти. *Економіка, управління та адміністрування.* 2021. № 2(96). С. 61–69.

2. Шишкова Н. Л. Засоби підвищення керованості безпекою облікової інформації. *Економічний вісник.* 2016. № 3. С. 119–127.

3. Ахрамович В. М., Амелькін С. В. Система захисту інформації приватного підприємства. Організація служби захисту інформації приватного підприємства. *Сучасний захист інформації*. 2019. № 1(37). С. 21–27.

4. Варічева Р. В. Захист інформаційних даних управлінського обліку: організаційно-кадрова складова. *Проблеми і перспективи економіки та управління.* 2015. № 3(3). С. 308–312.

5. Осмятченко В. О., Склярук І. П. Сучасні ІТ-рішення для обліку та управління бізнесом. *Підприємництво і торгівля.* 2022. № 34. С. 41–46.

6. Скрипник С. В., Франчук І. Б., Шепель І.В. Особливості автоматизації обліку підприємств в сучасних умовах. *Економіка та держава*. 2020. № 10. С. 39–45.

7. Ясінська А.І. Проблеми та перспективи електронного документообігу в умовах цифрової трансформації. *Молодий вчений*. 2022. № 11(111). С. 128–134.

8. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 22.11.2023).

9. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 22.11.2023).

10. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/go/2297-17 (дата звернення: 22.11.2023).

11. Про перелік відомостей, ще не становлять комерційної таємниці: Постанова КМУ від 09.08.1993 р. № 61. URL: https://zakon.rada.gov.ua/go/611-93-%D0BF (дата звернення: 22.11.2023).

12. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IУ. URL: https://zakon.rada.gov.ua/laws/show/436-15 (дата звернення: 22.11.2023).

13. Господарський кодекс України: Закон України від 16.01.2003 р. № 436-IУ. URL: https://zakon.rada.gov.ua/laws/show/436-15 (дата звернення: 22.11.2023).

REFERENCES:

1. Lehenchuk S. F., Nazarenko T. P., Tsaruk I. M. (2021). Pryntsypy zakhystu danykh u sysytemi obliku: upravlinski aspekty [Principles of data protection in the accounting system: management aspects]. *Ekonomika, upravlinnia ta administruvannia*. Vol. 2(96), pp. 61–69. [in Ukrainian]

2. Shyshkova N. L. (2016). Zasoby pidvyshennia kerovanosti bezpekoiu oblikovoi informatsii [Means to improve the controllability of accounting information security]. *Ekonomichnyi visnyk.* Vol. 3, pp. 119–127. [in Ukrainian]

3. Akhramovych V. M., Amelkin S. V. (2019). Systema zakhystu informatsii pryvatnoho pidpryiemstva. Orhanizatsiia sluzhby zakhystu informatsii pryvatnoho pidpryiemstva [Information security systems for private enterprise. Organization of the information security service of a private enterprise]. *Suchasnyi zakhyst informatsii*. Vol. 1(37), pp. 21–27. [in Ukrainian]

4. Varicheva R. V. (2015). Zakhyst informatsiinykh danykh upravlinskoho obliku: orhanizatsiino-kadrova skladova [Protection of information data of management accounting: the organizational and personnel component]. *Problemy i perspektyvy ekonomiky ta upravlinnia.* Vol. 3(3), pp. 308–312. [in Ukrainian]

5. Osmiatchenko V. O., Skliaruk I. P. (2022). Suchasni IT-rishennia dlia obliku ta upravlinnia biznesom [Modern IT solutions for accounting and business management]. *Pidpryiemnytsvo i torhivlia.* Vol. 34, pp. 41–46. [in Ukrainian]

6. Skrypnyk S. V., Franchuk I. B., Shepel I. V. (2020). Osoblyvosti avtomatyzatsii obliku pidpryiemstv v suchasnykh umovakh [Features of automation of enterprise accounting in modern conditions]. *Ekonomika ta derzhava*. Vol. 10, pp. 39–45. [in Ukrainian]

7. Yasinska A. I. (2022). Problemy ta perspektyvy elektronnoho dokumentoobihu v umovakh tsyfrovoi transformatsii [Problems and prospects of electronic document management in the context of digital transformation]. Molodyi vchenyi. Vol. 11(111), pp. 128–134. [in Ukrainian]

8. On access to public information: Law of Ukraine № 2939-VI (2011) Vidomosti Verkhovnoyi Rady Ukrayiny. Available at: https://zakon.rada.gov.ua/laws/show/2939-17 (accessed November 22, 2023).

9. About information: Law of Ukraine № 2657-XII (1992) Vidomosti Verkhovnoyi Rady Ukrayiny. Available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text (accessed November 22, 2023).

10. On the protection of personal data: Law of Ukraine № 2297-VI (2010) Vidomosti Verkhovnoyi Rady Ukrayiny. Available at: https://zakon.rada.gov.ua/go/2297-17 (accessed November 22, 2023).

11. On the list of information that does not constitute a commercial secret: Resolution of the Cabinet of Ministers of Ukraine № 61 (1993). Available at: https://zakon.rada.gov.ua/go/611-93-%D0BF (accessed November 22, 2023).

12. Tsyvilnyi kodeks Ukrainy: Kodeks Ukrainy vid 16.01.2003 No. 435-IV [Civil Code of Ukraine: Code of Ukraine dated 16.01.2003 No. 435-IV]. Available at: https://zakon.rada.gov.ua/laws/show/436-15#Text (accessed November 22, 2023).

13. Hospodarskyi kodeks Ukraine: Kodeks Ukraine vid 16.01.2003 No. 436-IV [Economic Code of Ukraine dated 16.01.2003 No. 436-IV]. Available at: https://zakon.rada.gov.ua/laws/show/436-15 (accessed November 22, 2023).