УДК 004.056.5:004.4’242:005.52
DOI https://doi.org/10.32782/tnv-tech.2025.2.23

АНАЛІЗ ТЕХНОЛОГІЙ ЗБЕРІГАННЯ КОНФІДЕНЦІЙНИХ ДАНИХ У CRM/ERP-СИСТЕМАХ УПРАВЛІННЯ БІЗНЕС-ПРОЦЕСАМИ ПІДПРИЄМСТВА

Чорненький М. В. *– аспірант Приватного вищого навчального закладу «Європейський університет»*
ORCID ID: 0009-0008-9321-4599

Скляренко О. В. *– кандидат фізико-математичних наук, доцент, завідувач кафедри математичних дисциплін та інноваційного проектування Приватного вищого навчального закладу «Європейський університет»*
ORCID ID: 0000-0001-6555-1223
Scopus-Author ID: 57192677216

У статті досліджуються системи CRM (Customer Relationship Management) / ERP (Enterprise Resource Planning) як усталені компоненти сучасних бізнес-процесів з акцентом на обсобливостях їхньої архітектури і, відповідно, перевагах та вразливостях, а також у фокусі необхідності вдосконалення засобів безпечного збереження конфіденційних даних і мінімізації ризиків несанкціонованого доступу до них. Метою дослідження є аналіз сучасних технологій зберігання та захисту конфіденційних даних у CRM/ERP-системах управління бізнес-процесами та надання практичних рекомендацій щодо підвищення безпеки зберігання інформації в умовах ескалації кіберзагроз. Результати дослідження демонструють, що порівняно з локальною та гібридною хмарна архітектура CRM/ERP-систем має переваги (автоматичні оновлення від провайдера, в тому числі безпекові, нижчі операційні видатки на утримання). Поза тим, надзвичайно серйозною загрозою безпечному зберіганню даних за допомогою CRM/ERP-систем є соціальна інженерія. Знизити цю загрозу дозволяють стандарти GDPR та ISO/IEC 27001. Але через певні технічні чинники (GDPR рідко оновлюється, ISO/IEC 27001 має рекомендативний характер) ці стандарти можуть вважатися лише одним із компонентів комплексної цифрової безпеки бізнесу. Для забезпечення збереження конфіденційності даних пропонується дотримуватися комплексної безпекової стратегії, яка має регулярно переглядатися відповідно до змін у ландшафті загроз і ризиків. Надано перелік ефективних заходів щодо підвищення безпеки збереження чутливих даних і наголошується на необхідності подальшої роботи з ідентифікації потенційних ризиків і пошуку шляхів їх нейтралізації.

Ключові слова: *CRM, ERP, кіберзагроза, зберігання конфіденційних даних, безпека хмарних рішень, соціальна інженерія, комплексна безпекова стратегія.*

Chornenkyi M. V., Skliarenko O. V. Analysis of confidential data storage technologies in CRM/ERP business process management systems of an enterprise

The article examines CRM (Customer Relationship Management) / ERP (Enterprise Resource Planning) systems as established components of modern business processes with an emphasis on the features of their architecture and, accordingly, advantages and vulnerabilities, as well as the need to improve the means of secure storage of confidential data and minimize the risks of unauthorized access to them. The purpose of the study is to analyze modern technologies for storing and protecting confidential data in CRM/ERP business process management systems and provide practical recommendations for improving the security of information storage in the context of escalating cyber threats. The results of the study demonstrate that the cloud architecture of CRM/ERP systems has advantages (automatic updates, including security updates, lower operating costs for maintenance). In addition, social engineering is an extremely serious threat to secure data storage using CRM/ERP systems. The GDPR and ISO/IEC 27001 standards can help mitigate this threat. However, due to technical factors (GDPR is rarely updated, ISO/IEC 27001 is advisory), these standards can only be considered one component of a comprehensive digital business security. To ensure data confidentiality is maintained, a comprehensive security strategy should be followed, which should be regularly reviewed in line with changes in the threat

and risk landscape. A list of effective measures to enhance the security of sensitive data storage is provided, with an emphasis on the need for further efforts to identify potential risks and explore ways to mitigate them.

Key words: *CRM, ERP, cyber threat, storage of confidential data, cloud security, social engineering, comprehensive security strategy.*

Постановка проблеми. У сучасному інформаційному суспільстві, сповненому економічних і цивілізаційних викликів, CRM (Customer Relationship Management) / ERP (Enterprise Resource Planning) системи стали невід'ємною частиною бізнес-процесів абсолютної більшості підприємств, що викликано прагненням, а, інколи, й необхідністю автоматизації та оптимізації операційної діяльності з метою здобуття конкурентної переваги та підвищення ефективності підприємства [8].

CRM-частина таких систем відповідає за поліпшення та автоматизацію роботи із замовниками, переймаючи на себе низку завдань, як-от [1]: збереження клієнтської бази (контакти, історія взаємодій, покупки тощо); автоматизація продажів (автоматичне оброблення та формування замовлень, нагадування менеджерам, контроль виконання завдань); покращення обслуговування клієнтів (швидкий доступ до інформації, персоналізація); маркетингова складова (e-mail-розсилки, аналітика кампаній і замовників); збір аналітичних даних задля покращення розуміння потреб клієнта та актуальних ринкових тенденцій.

ERP-частина систем відповідає за об'єднання різних підрозділів компанії, процесів, виробничих практик і політик, які в ній застосовуються, в єдиний синхронізований потік із метою подальшого їх контролю та автоматизації. До цієї частини входять [1]: автоматизація облікових процесів (фінанси, бухгалтерія, податки); керування, моніторинг і планування ресурсів підприємства (наявна техніка – виробнича, офісна і т. ін., персонал тощо); складські відомості (наявність продуктів на складі, їх розташування та кількість); спрощення ведення логістичних відомостей; координація, контроль і планування виробництва; каталогізація товарів і послуг.

Підсумовуючи вищевикладене, розглянуті системи містять багато чутливої інформації, а саме: персональні дані клієнтів; дані постачальників, що можуть становити комерційну таємницю; конфіденційні відомості про виробничі практики, фінансові операції тощо. Через неправильне використання технологій зберігання чи прогалини в системах безпеки такі дані можуть потрапити до третіх осіб і заподіяти непоправну шкоду підприємству, його клієнтам чи постачальникам.

Отже, проблематика дослідження полягає в необхідності забезпечення безпечного збереження зазначених вище конфіденційних даних і мінімізації ризику отримання цих даних третіми особами.

Аналіз останніх досліджень і публікацій. У сучасних наукових і фахових публікаціях особлива увага приділяється питанням безпечного захисту конфіденційних даних у системах CRM/ERP як основі управління бізнес-процесами в компанії. Розглянемо основні напрями досліджень і запропоновані шляхи вирішення даної проблеми.

Різноманітні дослідження, вказують на зростання популярності хмарних ERP/CRM-додатків і, як наслідок, підвищення загроз, пов'язаних зі зберіганням даних і віддаленим доступом до них. Основними заходами безпеки хмарних рішень ERP/CRM є шифрування даних «у стані спокою» і «в русі» та розділення прав доступу.

Чимало публікацій присвячено запровадженню стандартів і правил у CRM/ERP-системах. Так, Бенджамін Мюллер у своєму дослідженні розглядає вплив

транскордонних нормативних актів (GDPR, ISO/IEC 27001, CCPA) на адаптацію та дизайн CRM/ERP, зазначає важливість вбудованої конфіденційності (за проєктом), де персональні дані захищені на етапі їх обробки [2].

Багато дослідників розглядають технічні засоби забезпечення безпеки [3], наприклад, використання симетричного та асиметричного шифрування (AES, RSA), токенізацію чутливих полів (номерів карток, імен клієнтів), використання багатофакторної автентифікації (MFA) в CRM/ERP.

У деяких статтях, присвячених реагуванню на інциденти та управління вразливістю, йдеться про вимогу періодичних перевірок безпеки та оновлень системи. Пропонується модель управління вразливістю з використанням системи SIEM (Security Information and Event Management) для виявлення аномалій у реальному часі [4].

У низці нещодавніх досліджень детально описують використання моделей штучного інтелекту (ШІ) для виявлення підтвердженої активності в системах CRM [3]. Натомість інші праці зосереджені на виробничих технологіях блокчейну для забезпечення незмінності журналів доступу до конфіденційних даних [4].

Проаналізовані дослідження підтверджують, що питання безпечного зберігання конфіденційної інформації в системах CRM/ERP є міждисциплінарним. Оптимальними вважаються багатопланові рішення, які включають технологічні засоби та відповідають нормативним вимогам. Утім, з огляду на невпинне зростання кількості та потужності кібератак, людський фактор і складність інтеграції безпечних рішень у наявну інфраструктуру проблема дотепер залишається актуальною [9, 10].

Протягом усієї нової ери цифрового бізнесу системи управління підприємством, зокрема CRM (Customer Relationship Management) та ERP (Enterprise Resource Planning), в основному відповідають за підтримання ефективності внутрішніх процесів і спілкування з клієнтами. Однак, з еволюціонуванням цих систем і розширенням можливостей, які вони надають користувачам, зростає й ризик, пов'язаний з обробкою та зберіганням конфіденційної інформації. Тому проблема захисту даних у таких інформаційних системах набуває стратегічного значення як з погляду технічної реалізації, так і в аспекті нормативно-правового регулювання.

Метою дослідження є аналіз сучасних технологій зберігання та захисту конфіденційних даних у CRM/ERP-системах управління бізнес-процесами підприємства та визначення практичних рекомендацій щодо впровадження ефективних заходів для забезпечення безпеки інформації в умовах ескалації кіберзагроз.

У рамках поставленої мети визначено такі основні завдання дослідження:

– проаналізувати основні технічні засоби та заходи захисту інформації, які використовуються для зберігання секретної інформації (шифрування, токенізація, автентифікація тощо);

– дослідити роль міжнародних стандартів і вимог (GDPR, ISO/IEC 27001);

– вивчити поточні загрози та вразливості CRM/ERP-систем і визначити, як можна їх нівелювати.

Отже, метою даної статті є не лише узагальнення наявних наукових підходів до збереження конфіденційної інформації в системах управління підприємствами, а й надання практичних рекомендації щодо адаптації цих підходів до вимог сучасного інформаційного середовища.

Виклад основного матеріалу. Як вже було відзначено вище, основними технічними засобами інформації є комплекс різних складових, що мають працювати в синергії задля досягнення бажаного результату. Основні засоби можна

розподіліти на декілька підкатегорій, а саме: засоби безпечного зберігання даних, засоби соціальної інженерії та засоби моніторингу захисту від кібератак [3].

До засобів безпечного зберігання даних можна віднести шифрування і токенізацію. Шифрування забезпечує перетворення даних у недоступний для неавторизованих користувачів формат. Серед основних типів шифрування можна виділити шифрування на рівні бази даних (зазвичай використовується для зберігання фінансових та клієнтських даних); транспортне шифрування (використовується для захисту даних, які передаються між клієнтом і сервером); асиметричні алгоритми (використовуються для захисту ключів автентифікації). Зазвичай цей аспект захисту доступний у ядрі CRM/ERP-системи і не потребує додаткових змін, окрім налаштувань залежно від потреб кінцевого клієнта.

Своєю чергою, токенізація – це метод збереження даних у форматі унікального маркера (зазвичай GUID ключ). У цьому випадку маркер не є зашифрованим значенням, він лише слугує ключем, за допомогою якого дані можуть бути отримані із захищеного місця за межами основної бази даних. Доступ до сховища таких даних потребує додаткової автентифікації, що зазвичай вбудована в CRM/ERP-систему. Одним із прикладів такого сховища виступає Isolated Storage від Microsoft [5].

Результатом використання цих засобів буде значне зниження ризику можливості використання вже отриманих конфіденційних даних через їхній невикористовуваний формат. Проте варто зауважити, що будь-які шифрування чи токенізації займають час, тож застосування цих підходів для абсолютно всіх даних значно знизить швидкість роботи системи. Це наштовхує на думку про необхідність глибокого аналізу даних і чіткого розподілення їх на конфіденційні та загальнодоступні для потенційного підвищення швидкодії системи.

Засоби соціальної інженерії покликані запобігти доступу зловмисників до даних за допомогою наявного користувача системи. Прикрий, але доведений факт полягає в тому, що нині абсолютна більшість кібератак починається саме із соціального зламу (підбору автентифікаційної інформації користувача, крадіжки пристою з наданим доступом, застосування фішингових програм тощо). До засобів соціальної інженерії включають контроль доступу, який дозволяє контролювати можливість і рівень доступу для кожного з користувачів. Детальніше цей інструмент можна описати так: контроль доступу необхідний для уникнення підозрілих активностей (користувач заходить із різних пристроїв / IP-адрес одночасно). Поряд із прямим моніторингом зазвичай системи можуть збирати інформацію про дії користувача в окремих логах, що потім можуть бути проаналізовані, задля запобігання подальшого використання системи сторонніми особами. Рівень доступу визначається роллю користувача в системі (якщо користувач працює в складському відділі, він не повинен мати доступу до фінансової інформації і т. ін.).

Багатофакторна автентифікація як засіб соціальної інженерії дає змогу мінімізувати ризики, пов’язані з можливістю підбору простих автентифікаційних даних чи крадіжки пристрою з наявним доступом до системи. Такі механізми є стандартом індустрії і можуть бути представлені в різних комбінаціях (автентифікаційні дані + відбиток пальця, сканування обличчя + код автентифікації, відправлений на інший пристрій тощо).

Засоби моніторингу захисту від кіберзагроз є комплексними інструментами, які запобігають несанкціонованому доступу до системи та витокам даних. Приміром, DLP (Data Loss Prevention) запобігає витоку даних через файлообмінники, e-mail тощо. Зазвичай DLP є інтеграцями з однією або декількома подібними зовнішніми системами. IDS/IPS (Institution Detection / Prevention Systems) сфокусовані

на виявленні спроб несанкціонованого доступу. Маючи таку інформацію, адміністратори системи можуть вжити заходів, які обмежать потенційного несанкціонованого користувача від доступу до системи (блокування на рівні Firewall, зміна портів тощо). Натомість інтелектуальні системи аналізу загроз використовують штучний інтелект (ШІ) задля виявлення аномалій у поведінці користувача системи, використання блокчейн-технології для збереження логів доступу з метою подальшого аудиту доступу.

Послуговуючись проаналізованими даними, цілком доречно буде розглянути наявні міжнародні стандарти та вимоги до збереження конфіденційних даних, адже, крім впливу на CRM/ERP-системи, базуючись на них та їх дотриманні, потенційний клієнт може приймати рішення про роботу з тим чи іншим бізнес-проєктом. На сьогодні основними та найчастіше використовуваними у Європі є Міжнародний стандарт ISO/IEC 27001 [6] та Загальний регламент про захист даних (GDPR) [7] (таблиця 1).

Таблиця 1

Порівняння GDPR та ISO/IEC 27001

Аспект	GDPR (ЄС)	ISO/IEC 27001 (міжнародний стандарт)
Об'єкт захисту	Персональні дані фізичних осіб (резидентів ЄС)	Уся інформація, яка потребує захисту (не лише персональні дані)
Обов'язковість впровадження	Обов'язковий для компаній, які обробляють персональні дані громадян ЄС	Добровільний, але рекомендований і часто вимагається партнерами
Ключові права користувача	Доступ, виправлення, видалення, обмеження обробки, портативність	Не регламентує права суб'єктів даних напряму
Механізми безпеки	Шифрування, аудит, контроль доступу, «privacy by design/ default»	Каталог заходів безпеки Annex A (93 контролі, що є конкретними кроками, які охоплюють різні аспекти безпеки)
Обов'язкове повідомлення про витік	Протягом 72 годин після виявлення	Залежить від внутрішніх процедур організації
Санкції за порушення	До 20 млн євро або 4 % глобального річного доходу	Відсутні; наслідки – втрата сертифіката або репутаційні ризики
Вплив на CRM/ ERP-системи	Необхідність впровадження функцій згоди, логування, видалення, обмеження доступу	Стандартизація процесів безпеки, регулярний аудит

Таблиця 1 ілюструє відмінності між GDPR та ISO/IEC 27001, ключовою з яких є та, що впровдження GDPR є обов'язковим для компаній, які базуються у ЄС або надають послуги громадянам ЄС (не є обов'язковим також для українських компаній, які не співпрацюють з ринком ЄС), натомість впровадження ISO/IEC 27001 носить лише рекомендаційний характер. Маючи на увазі, що стандарт GDPR є обов'язковим до дотримання у ЄС, його основними проблемами постають швидкість і частота оновлення, адже востаннє це відбулося у 2018 році, що в хронології ІТ-всесвіту є неймовірно віддаленим у часі періодом. Своєю чергою,

ISO/IEC 27001 оновлюється частіше і є більш актуальним, проте, як вже зазначалося вище, має радше рекомендаційний характер.

Спираючись на основні технічні заходи для захисту інформації, міжнародні стандарти та вимоги, необхідно розглянути поточні загрози та вразливості CRM/ERP-систем. Наразі наявні різні типи реалізації CRM/ERP-систем, а саме: локальна архітектура (система встановлюється та функціонує на серверах підприємства, тож повний контроль і відповідальність покладено на це підприємство); хмарна архітектура (система встановлена в хмарному середовищі, яке повністю або частково керується зовнішнім провайдером); гібридна архітектура (поєднання двох описаних вище архітектур з відповідно розподіленою відповідальністю).

В умовах сьогодення загрози для CRM/ERP-систем можуть змінюватися залежно від типу архітектури (таблиця 2).

Таблиця 2

Загрози та вразливості CRM/ERP-систем залежно від типу архітектури

Архітектура	Типові вразливості	Ключові загрози	Особливості безпеки
Локальна	Застарілі ПЗ та/або ОС; відсутність автоматичних оновлень; слабка внутрішня ізоляція; непрозорість журналів	Несанкціонований фізичний доступ; віруси через USB/ мережу; помилки IT-персоналу; еомпрометація даних авторизації; витоки через сторонні сервіси	повний контроль над інфраструктурою; підвищені витрати на захист; обмежений захист від DDoS
Хмарна	Неправильне налаштування доступу (ACL, IAM); Уразливості API; Відсутність видимості	Витоки через сторонні сервіси; Атаки через спільну хмарну інфраструктуру; Компроментація даних авторизації	Вбудовані механізми безпеки від провайдера; Часті оновлення; Менше контролю з боку користувача та організації
Гібридна	Розрив між локальною та хмарною безпекою; неузгоджені політики; низька інтеграція моніторингу	Міжмережеве проникнення; уразливості при передачі даних між середовищами API-залежності; компрометація даних авторизації; витоки через сторонні сервіси	Потреба в чіткій сегментації даних; високий ризик конфігураційних помилок; складність проведення аудиту

Як результат проведеного порівняння небезпек можна відмітити, що найскладнішими в захисті є системи з гібридним типом архітектури через особливості їхньої структури і необхідність одночасного контролю багатьох параметрів. Усі три архітектури мають спільні вразливості, пов’язані із соціальною інженерією. Локальна та хмарна архітектури мають свої слабкі та сильні сторони, проте, за підсумками аналізу, варто відмітити, що хмарна архітектура виглядає набагато більш виграшно через часті автоматичні оновлення від провайдера (які в тому

числі включатимуть безпекові оновлення) та нижчі операційні видатки на утримання такої системи.

Висновки. У даній статті було проведено комплексне дослідження засобів безпечного зберігання даних, наявних стандартів захисту даних, загроз і вразливостей. За результатами дослідження можна зробити такі узагальнення.

Окрім технічних небезпек і вразливостей, надзвичайно серйозну загрозу для збереження конфіденційних даних становить соціальна інженерія.

Стандарти GDPR та ISO/IEC 27001 є важливою складовою безпеки CRM/ERP-систем, проте через рідкість оновлення GDPR і рекомендативний характер ISO/IEC 27001 вони мають бути основою безпеки, але аж ніяк не повною та вичерпною її формою.

Залежно від типу архітектури системи наявні різні технічні відмінності в захисті та убезпеченні від потенційних загроз.

Як висновок, потрібно зазначити, що для збереження конфіденційності даних слід дотримуватися комплексної безпекової стратегії, яка включатиме: проведення безпекових тренінгів для персоналу, аудиту та моніторингу робочих процесів з метою мінімізації ризиків, пов'язаних із соціальною інженерією; аналіз структури даних та потенційну токенізацію / шифрування; використання систем моніторингу кібератак та захисту від них; дотримання стандартів GDPR та ISO/IEC 27001 як частини безпекової політики; незалежно від архітектури системи підтримання її безпекової актуальності за допомогою регулярних оновлень; регулярний контроль потенційних загроз, притаманних тій чи іншій архітектурі.

Перспективи подальших досліджень охоплюють розгляд потенційних ризиків і шляхів захисту від них, нових стандартів і підходів до побудови архітектури CRM/ERP-систем. Подальший аналіз сприятиме розробленню нових практик захисту та глибшому розумінню ризиків, які будуть унаочнені й атрибутовані завдяки IT-можливостям майбутнього, але є актуальним вже сьогодні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Gartner Magic Quadrant for Cloud ERP for Product-Centric Enterprises. 2023. URL: https://www.gartner.com/en/documents/4800931 (дата звернення: 24.04.2025).

2. Lobschat L., Mueller B., Eggers F. et al. Corporate digital responsibility. *Journal of Business Research*. 2021. Vol. 122. P. 875–888.

3. Cloud Security Alliance (CSA). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. 2021. URL: https://cloudsecurityalliance.org (дата звернення: 24.04.2025).

4. OWASP Foundation. OWASP Top 10: The Ten Most Critical Web Application Security Risks. URL: https://owasp.org/www-project-top-ten/ (дата звернення: 24.04.2025).

5. Microsoft. Dynamics 365 Security Whitepaper. 2023. URL: https://learn.microsoft.com (дата звернення: 24.04.2025).

6. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Edition 3. Geneva : International Organization for Standardization, 2022. 19 p.

7. Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data. URL: https://gdpr.eu (дата звернення: 24.04.2025).

8. Скляренко О. В., Федік О. І., Колодінська Я. О. Digital рішення для управління проектами та бізнес-процесами в умовах сучасних викликів. *Економіка і управління*. 2021. № 2. С. 85–90. URL: https://e-u.edu.ua/journal/1088.pdf (дата звернення: 24.04.2025).

9. Яровий Р., Улічев О., Скляренко О., Пашорін В. Моделювання мультиагентних систем захисту інформаційних ресурсів. *Вісник Хмельницького національного університету. Технічні науки*. 2024. № 3 (2) (337). С. 278–284. URL: https://doi.org/10.31891/2307-5732-2024-337-3-42 (дата звернення: 24.04.2025).

10. Дмитрик І. О., Загороднюк О. В. Роль BPM, CRM та ERP систем у цифровій трансформації українського бізнесу. *Вісник Уманського національного університету садівництва*. 2024. Вип. 104.2. С. 191–201. URL: http://journal.udau.edu.ua (дата звернення: 24.04.2025).

REFERENCES:

1. Gartner Magic Quadrant for Cloud ERP for Product-Centric Enterprises. 2023. Retrieved from: https://www.gartner.com/en/documents/4800931.

2. Lobschat L., Mueller B., Eggers F. et al. (2021). Corporate digital responsibility. *Journal of Business Research*. 122: 875–888.

3. Cloud Security Alliance (CSA). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. 2021. Retrieved from: https://cloudsecurityalliance.org.

4. OWASP Foundation. OWASP Top 10: The Ten Most Critical Web Application Security Risks. Retrieved from: https://owasp.org/www-project-top-ten/.

5. Microsoft. Dynamics 365 Security Whitepaper. 2023. Retrieved from: https://learn.microsoft.com.

6. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Edition 3. (2022). Geneva: International Organization for Standardization. 19 p.

7. Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data. Retrieved from: https://gdpr.eu.

8. Skliarenko, O. V., Fedik, O. I., & Kolodinska, Y. O. (2021). Digital solutions for project and business process management in the context of modern challenges. *Economics and Management*, 2, 85–90 [in Ukrainian].

9. Yarovyi, R., Ulichev, O., Skliarenko, O., & Pashorin, V. (2024). Modeling of multi-agent systems for protecting information resources. *Herald of Khmelnytskyi National University. Technical Sciences*, 337 (3(2)), 278–284. Retrieved from: https://doi.org/10.31891/2307-5732-2024-337-3-42 [in Ukrainian].

10. Dmytryk, I. O., & Zahorodniuk, O. V. (2024). The role of BPM, CRM and ERP systems in the digital transformation of Ukrainian business. *Bulletin of Uman National University of Horticulture*, 104.2, 191–201. Retrieved from http://journal.udau.edu.ua [in Ukrainian].