DOI: https://doi.org/10.32782/2524-0072/2024-64-111

УДК 005.6

ІНТЕГРАЦІЯ СИСТЕМ І ЗАХИСТ ІНФОРМАЦІЇ ЯК НАПРЯМИ УДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ СЕРЕДОВИЩЕМ ПІДПРИЄМСТВА В УМОВАХ ДІДЖИТАЛІЗАЦІЇ

INTEGRATION OF SYSTEMS AND INFORMATION SECURITY AS AREAS FOR IMPROVING THE MANAGEMENT OF THE ENTERPRISE INFORMATION ENVIRONMENT IN THE CONTEXT OF DIGITALIZATION

Орєхова Альвіна Іванівна
доктор економічних наук, професор,
Сумський національний аграрний університет
ORCID: https://orcid.org/0000-0003-1016-3287

Харченко В'ячеслав Вікторович
аспірант,
Сумський національний аграрний університет
ORCID: https://orcid.org/0009-0002-9450-8149

Oriekhova Alvina, Kharchenko Viacheslav
Sumy National Agrarian University

Стаття присвячена дослідженню найбільш важливих аспектів, пов'язаних з інтеграцією систем та інформаційною безпекою. Інтеграція систем означає з'єднання різних інформаційних систем підприємства. Основною метою інтеграції систем в умовах діджиталізації є створення єдиного інформаційного середовища, де всі дані зберігаються та обробляються централізовано, забезпечується своєчасний і точний доступ до них для всіх користувачів. Важливим аспектом покращення управління інформаційним середовищем є забезпечення безпеки даних. Це включає використання сучасних технологій шифрування, багатофакторної аутентифікації та інших засобів захисту інформації. Інтеграція систем та захист інформації разом створюють основу для успішної діджиталізації бізнесу, підвищуючи його ефективність і здатність адаптуватися до постійних змін ринкових умов і технологічних інновацій.

Ключові слова: управління, інформаційне середовище, інтеграція систем, захист інформації, діджиталізація.

The article is devoted to the study of the most important aspects related to systems integration and information security in the context of improving the management of an enterprise's information environment. Systems integration means connecting various information systems and software applications of an enterprise so that they work as a single, coordinated mechanism. The main goal of systems integration is to create an information environment where all data is stored and processed centrally, and timely and accurate access to it is provided for all users. One of the most common examples is the integration of an ERP system with a CRM system. The integration of these two systems allows to automatically transfer customer and order data between them. This ensures a faster and more accurate order fulfillment process, reduces the risk of errors, and reduces or eliminates manual data entry. The key advantage of integrating systems in a digitalized environment is increased efficiency and accuracy of information. An important aspect of improving information environment management along with system integration is ensuring data security and confidentiality. This includes the use of modern encryption technologies, multi-factor authentication and other security tools. Enterprise information security is a set of measures and technologies aimed at ensuring the integrity, confidentiality and availability of data. Security monitoring and auditing are critical elements in ensuring information security. Continuous monitoring of network activity allows to detect suspicious activities or anomalies that may indicate cyberattacks or data leaks. Regular security audits, which can be conducted by both internal specialists and external auditors, help assess the effectiveness of existing security measures, identify

vulnerabilities, and identify areas for improvement. Integration of systems and information security together create the basis for successful business digitalization, increasing its efficiency and ability to adapt to constant changes in market conditions and technological innovations.

Keywords: management, information environment, systems integration, information security, digitalization.

Постановка проблеми. Поєднання інтеграції систем і захисту інформації створює потужну платформу для покращення управління інформаційним середовищем підприємства. З одного боку, інтеграція забезпечує безперервний обмін даними, що підвищує ефективність бізнес-процесів і дозволяє отримувати більш точну та своєчасну аналітику. З іншого боку, захист інформації гарантує, що ці дані залишаються безпечними та захищеними від будь-яких загроз. Такий комплексний підхід да можливість підприємствам не лише підвищити продуктивність і знизити витрати, але й забезпечити стійкість і надійність їх інформаційного середовища. Отже, прикладні аспекти впровадження даних напрямів покращення є важливими з точки зору якості інформаційного менеджменту та в умовах діджиталізації набувають першочергового значення. Все це зумовлює експертний інтерес до визначеної теми дослідження та доводить її наукову новизну і актуальність.

Аналіз останніх досліджень і публікацій. нтеграція систем досліджується багатьма авторами. Зокрема, у роботах [2; 3; 5] та [7] фокусується увага на певних заходах та/або засобах, спрямованих на покращення управління. Захист інформації висвітлюється у роботах [1; 4; 6] та [8]. Але дослідженню як першого, так і другого аспектів бракує конкретики щодо практичного їх застосування в умовах діджиталізованого інформаційного середовища й особливо прикладів такого застосування.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження найбільш важливих організаційних аспектів, пов’язаних із інтеграцією систем і захистом інформації в контексті покращення управління інформаційним середовищем підприємства в умовах діджиталізації.

Виклад основного матеріалу дослідження. В сфері інформаційних технологій існує проблема інтеграції декількох відокремлених систем [3, с.36]. Інтеграція систем означає з'єднання різних інформаційних систем і програмних додатків підприємства, щоб вони працювали як єдиний, узгоджений механізм. Це процес, який дозволяє різним системам обмінюватися даними та функціонувати в рамках діджиталізованої інформаційної інфраструктури, що значно підвищує ефективність бізнес-процесів і зменшує ризик помилок та дублювання даних. Основною метою інтеграції систем в умовах діджиталізації є створення єдиного інформаційного середовища, де всі дані зберігаються та обробляються централізовано, забезпечується своєчасний і точний доступ до них для всіх користувачів та систем. Це досягається за допомогою різних технологій та методів інтеграції, включаючи програмні інтерфейси (API), шлюзи даних, об'єднані бази даних та інші інструменти, що дозволяють автоматизувати обмін даними між різними системами. В результаті злиття інформаційний систем в єдиний інформаційний комплекс [7, с. 116] можлива безліч варіантів їх кінцевого стану.

Вирішенням проблем інтеграції різних спеціалізованих програм управління підприємством займаються системні інтегратори, тобто фахівці та фірми, котрі аналізують використовуване програмне забезпечення, оцінюють наявне на ринку програмне забезпечення та, ґрунтуючись на завданнях і фінансових можливостях клієнта, пропонують комплекс технічного й програмного забезпечення, налаштовують програми й перехідні модулі, навчають співробітників [5].

Одним з найбільш поширених прикладів в менеджменті є інтеграція ERP-системи з CRM-системою. ERP-система займається управлінням основними бізнес-процесами, такими як виробництво, постачання, фінанси та переміщення запасів. CRM-система, зі свого боку, фокусується на взаємодії з клієнтами, продажах, маркетингу та післязбутовій підтримці. Інтеграція цих двох систем в умовах діджиталізації дозволяє автоматично передавати дані про клієнтів і замовлення між ними. Тобто, коли нове замовлення вводиться в CRM-систему, воно автоматично оновлюється в ERP-системі, де може бути оброблене для управління запасами та виробництвом. Це забезпечує більш швидкий і точний процес виконання замовлень, знижує ризик помилок та скорочує або зовсім усуває ручне введення даних, таким чином зберігається актуальність інформації у реальному часі.

Інтеграція систем в умовах діджиталізації також може включати об'єднання різних платформ і додатків, таких як бухгалтерські програми, автоматизація управління запасами, виробничі системи, засоби з управління людськими ресурсами та інші. Це дозволяє створити єдину точку доступу до всієї необхідної інформації, що полегшує управління бізнесом і прийняття рішень. Крім того, інтеграція дозволяє отримувати більш повну та детальну аналітику, об'єднуючи дані з різних джерел в єдиний звіт.

Ключовою перевагою інтеграції систем в умовах діджиталізації є підвищення оперативності та точності інформації. Завдяки автоматизованому обміну даними між системами, інформація оновлюється у реальному часі, що дозволяє оперативно реагувати на зміни та приймати більш обґрунтовані рішення. Інтеграція також допомагає уникнути дублювання даних і зменшує кількість помилок, пов'язаних з ручним введенням інформації. Інтеграція систем в умовах діджиталізації сприяє покращенню комунікації та співпраці між різними відділами організації. Завдяки єдиному інформаційному середовищу, співробітники мають доступ до актуальної інформації, що полегшує координацію дій і підвищує ефективність їх роботи.

Інтеграція систем управління постачаннями та систем управління запасами є ще одним прикладом, який може значно оптимізувати бізнес-процеси. Дані про наявність товарів на складах, залишки запасів та потреби у поповненні автоматично оновлюються та передаються міжсистемами. Це дозволяє забезпечити своєчасне поповнення запасів, уникнути дефіциту або надлишку товарів і оптимізувати операційні витрати на складське зберігання. Управління запасами стає більш ефективним і прозорим, адже скорочуються чи зовсім зникають затримки у виконанні замовлень. Таким чином, підвищується рівень обслуговування клієнтів.

Інший приклад інтеграції стосується системи управління людськими ресурсами (HRMS) та системи управління часом і присутністю. Інтеграція цих систем дозволяє автоматизувати процеси обліку робочого часу співробітників, обчислення заробітної плати та управління відпустками. Дані про відпрацьований час і присутність автоматично передаються з системи управління часом до HRMS, що формує об’єктивні підстави для точного та своєчасного нарахування заробітної плати. Така інтеграція знижує ризик помилок у розрахунках, покращує управління персоналом та підвищує задоволеність співробітників завдяки своєчасній виплаті зарплат.

Ще один приклад – інтеграція системи управління проектами з фінансовою системою підприємства. Це дозволяє автоматично передавати дані про витрати, бюджети та фінансові показники проектів між такими системами. Управління проектами стає більш прозорим і контрольованим, оскільки фінансові дані постійно оновлюються і стають доступними для аналізу в реальному часі. Така інтеграція допомагає керівникам проектів та фінансовим менеджерам краще контролювати витрати, планувати бюджети та приймати обґрунтовані рішення з оптимізації проектного управління.

Інтеграція систем управління документообігом з іншими корпоративними системами також може значно підвищити ефективність роботи. Наприклад, інтеграція системи управління документообігом з ERP-системою дозволяє автоматично обробляти та зберігати документи, пов'язані з фінансовими транзакціями, замовленнями та іншими бізнес-процесами. Це також дає можливість централізовано зберігати документи, забезпечує легкий доступ до них, зменшує кількість паперової роботи та покращує контроль.

Інтеграція систем на даному етапі діджиталізації може включати використання хмарних технологій, призначених для зберігання та обробки даних у хмарі. Це забезпечує гнучкість і масштабованість інформаційної інфраструктури, сприяє зниженню витрат на апаратне забезпечення та надає доступ до документів з будь-якої точки світу. Хмарні рішення підвищують надійність та доступність даних, уможливлюючи їх резервне копіювання та відновлення втраченої інформації у разі збоїв або аварій.

Використання хмарних технологій у багаторівневій системі управління може значно удосконалити та осучаснити її роботу, підвищити ефективність, розподілити та пришвидшити обчислення, що базуються на інтегрованих даних, спростити створення єдиного інформаційного середовища [2, с. 25].

Важливим аспектом покращення управління інформаційним середовищем поряд з інтеграцією систем є забезпечення безпеки та конфіденційності даних. Адже під час інтеграції систем необхідно також враховувати захист інформації від несанкціонованого доступу, збереженняїї цілісності та відповідність правовим вимогам щодо захисту пер-

сональних даних. Це включає використання сучасних технологій шифрування, багатофакторної аутентифікації та інших засобів захисту інформації.Тому захист інформації на підприємстві є комплексом заходів і технологій, спрямованих на забезпечення цілісності, конфіденційності та доступності даних. При їх впровадженні потрібно також зважати [4, с. 112], що існує традиційний компроміс між безпекою, простотою використання, вартістю, складністю тощо. Отже, захист даних – критично важливий аспект діджиталізації, оскільки цифрова інформація є цінним активом, який може стати об'єктом різноманітних загроз, включаючи кіберзлочинність, внутрішні витоки та технічні збої.

Відтак, організація ефективних систем захисту корпоративної інформації на вітчизняних підприємствах сьогодні виступає об'єктивною необхідністю, яка забезпечує не лише необхідний і достатній рівень конкурентоспроможності й успіх в конкурентній боротьбі, але й саме виживання підприємства [8, с. 57].

Початковим етапом захисту інформації є ідентифікація всіх категорій даних, які потребують захисту. Це включає конфіденційні дані клієнтів, фінансові звіти, внутрішні документи підприємства та будь-яку іншу інформацію, яка має критичне значення для функціонування компанії. Після визначення категорій даних необхідно розробити стратегію їх захисту, що враховує специфічні потреби та ризики кожної категорії.

Один з ключових елементів захисту інформації полягає у використанні сучасних технологій шифрування. Шифрування даних як під час їхнього зберігання, так і під час передачі спрямовується на позбавлення можливості зловмисникам прочитати або використати інформацію навіть у випадку несанкціонованого доступу. Для цього застосовуються різні методи шифрування, зокрема симетричне та асиметричне шифрування, а також протоколи захищеного зв'язку, такі як SSL/TLS.

Багатофакторна аутентифікація є ще одним важливим елементом захисту інформації. Цей метод вимагає від користувачів надання двох або більше доказів своєї ідентичності перед отриманням доступу до систем або даних. Зазвичай це комбінація пароля та додаткового фактору, такого як код з мобільного додатку або біометричні дані. Багатофакторна аутентифікація значно знижує ризик несанкціонованого доступу, навіть якщо пароль буде скомпрометовано.

Моніторинг і аудит безпеки є критичними елементами для забезпечення захисту інформації. Постійний моніторинг мережевої активності дозволяє виявляти підозрілі дії або аномалії, що можуть свідчити про кібератаки або витоки даних. Регулярні аудити безпеки, які можуть проводитися як внутрішніми фахівцями, так і зовнішніми аудиторами, допомагають оцінити ефективність існуючих заходів захисту, виявити вразливості та визначити області для покращення. Захист від шкідливого програмного забезпечення включає використання антивірусних програм, брандмауерів, систем виявлення вторгнень та інших програмних засобів, що запобігають проникненню та поширенню вірусів, шпигунського ПЗ та інших типів шкідливих програм. Ці засоби повинні регулярно оновлюватися для забезпечення захисту від нових загроз.

Навчання персоналу є важливим аспектом загальної стратегії захисту інформації. Співробітники мають бути добре обізнані про основні принципи інформаційної безпеки, такі як використання складних паролів, розпізнавання фішингових атак та безпечне поводження з конфіденційною інформацією. Регулярні тренінги та освітні програми допомагають формувати усталену культуру кібербезпеки на підприємстві. Потребує актуалізації також уся система підготовки спеціалістів із безпеки [1, с.107], бо постає питання щодо компетентності персоналу, який розуміється лише на давно відомих способах порушення захисту баз даних.

Політика управління доступом визначає, хто і до яких даних має доступ. В умовах діджиталізації вона включає розподіл прав доступу на основі ролей та обов'язків співробітників, а також застосування принципу мінімальних привілеїв, що означає надання доступу лише до тих даних, які необхідні для виконання конкретних завдань. Такий підхід допомагає знизити ризик внутрішніх витоків та несанкціонованого втручання. Важливим аспектом захисту інформації є також розробка планів реагування на інциденти. Ці плани визначають дії, які необхідно вжити у разі виявлення порушень безпеки або витоків даних. Вони включають процедури виявлення інцидентів, їхнього аналізу, локалізації, ліквідації наслідків та відновлення нормальної роботи систем. Належним чином розроблений план реагування на інциденти допомагає мінімізувати збитки та швидко відновити функціонування інформаційного середовища підприємства.

Висновки. Інтеграція систем та захист інформації виступають як дві сторони однієї

медалі, що взаємодоповнюють одна одну і спільно сприяють покращенню управління інформаційним середовищем підприємства. Інтегровані системи забезпечують безперебійний потік інформації та автоматизацію процесів, тоді як заходи захисту інформації гарантують безпеку цих даних. Разом вони створюють основу для успішної діджиталізації бізнесу, підвищуючи його ефективність і здатність адаптуватися до постійних змін ринкових умов і технологічних інновацій. Таким чином, зростає конкурентоспроможність компанії та стабілізуються її перспективи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Антоненко Н.В., Граболюк М.С., Семенченко Н.О. Проблеми захисту інформації в сучасних базах даних. *Науковий вісник Полтавського університету економіки і торгівлі. Серія : Економічні науки.* 2021. № 2(1). С. 106–110.

2. Гречанінов В. Ф., Оксанич І.М., Лопушанський А.В. Використання хмарних технологій для вирішення питань інтеграції інформації у багаторівневих системах управління. *Controlsystems&computers.* 2022. № 4. С. 24–34.

3. Дивак Ю. А. Аналітичний огляд підходів до інтеграції програмних систем. *Проблеми програмування.* 2021. № 1. С. 36–48.

4. Довгаль Ю. С. Особливості побудови захисту інформаційних систем. *Науковий вісник публічного та приватного права.* 2016. Вип. 4. С. 111–115.

5. Мороз С. І., Нужна С. А. Інтеграція інформаційних систем і технологій у побудові інформаційного простору сільськогосподарських підприємств. *Ефективна економіка*[Електронний ресурс]. 2021. № 5. URL: http://www.economy.nayka.com.ua/?op=1&z=8897 (дата звернення: 23.07.2024).

6. Роєва О.С. Вплив інтеграційних процесів обліку на систему інформаційного забезпечення підприємства. *Проблеми системного підходу в економіці.* 2018. Вип. 5. С. 199–203.

7. Сахно Є. Ю., Скітер І. С., Двоєглазова М. В. Формування узагальненої моделі інтеграції інформаційних систем підприємства та проекту. *Управління розвитком складних систем.* 2013. Вип. 14. С. 116–121.

8. Чубаєвський В. І., Богма О. С., Сілакова Г. В. Методика оцінки ефективності систем захисту корпоративної інформації вітчизняних підприємств. *Економічний простір.* 2022. № 177. С. 56–61.

REFERENCES:

1. Antonenko, N. V., Hraboliuk, M. S. and Semenchenko, N. O. (2021) Problemy zakhystu informatsii v suchasnykh bazakh danykh [Problems of information security in modern databases]. *Naukovyi visnyk Poltavskoho universytetu ekonomiky i torhivli. Seriia :Ekonomichni nauky – Scientific Bulletin of Poltava University of Economics and Trade. Series: Economic sciences,* vol. 2(1), pp. 106–110.

2. Hrechaninov, V. F., Oksanych, I. M. and Lopushanskyi A. V. (2022) Vykorystannia khmarnykh tekhnolohii dlia vyrishennia pytan intehratsii informatsii u bahatorivnevykh systemakh upravlinnia [Using cloud technologies to solve information integration issues in multi-level management systems]. *Control systems & computers,* vol. 4, pp. 24–34.

3. Dyvak, Yu. A. (2021) Analitychnyi ohliad pidkhodiv do intehratsii prohramnykh system [Analytical review of approaches to software systems integration]. *Problemy prohramuvannia – Programming problems,* vol. 1, pp. 36–48.

4. Dovhal, Yu. S. (2016) Osoblyvosti pobudovy zakhystu informatsiinykh system [Features of building information system protection]. *Naukovyi visnyk publichnoho ta pryvatnoho prava – Scientific Bulletin of Public and Private Law,* vol. 4, pp. 111–115.

5. Moroz, S. and Nuzhna, S. (2021) Intehratsiia informatsiinykh system I tekhnolohii u pobudovi informatsiinoho prostoru silsko hospodarskykh pidpryiemstv [Integration of information systems and technologies in construction of information space of agricultural enterprises]. *Efektyvna ekonomika – Efficient economy* [Online], vol. 5. Available at: http://www.economy.nayka.com.ua/?op=1&z=8897 (accessed July 23, 2024).

6. Roieva, O. S. (2018) Vplyv intehratsiinykh protsesiv obliku na system informatsiinoho zabezpechennia pidpryiemstva [Impact of accounting integration processes on the enterprise information system]. *Problemy systemnoho pidkhodu v ekonomitsi - Problems of the systemic approach in the economy,* vol. 5, pp. 199-203.

7. Sakhno, Ye. Iu., Skiter, I. S. and Dvoiehlazova, M. V. (2013) Formuvannia uzahalnenoi modeli intehratsii informatsiinykh system pidpryiemstva ta proektu [Formation of a generalized model of integration of enterprise and project information systems]. *Upravlinnia rozvytkom skladnykh system – Managing the development of complex systems,* vol. 14, pp. 116–121.

8. Chubaievskyi, V.I., Bohma, O.S. and Silakova, H.V. (2022) Metodyka otsinky efektyvnosti system zakhystu korporatyvnoi informatsii vitchyznianykh pidpryiemstv [Methodology for assessing the effectiveness of corporate information security systems of domestic enterprises]. *Ekonomichnyi prostir – Economic space,* vol. 177, pp. 56–61.