З огляду на стрімкий розвиток технологій та зміну ландшафту загроз, компанії повинні залишатися гнучкими і готовими адаптувати свої стратегії кібербезпеки до нових викликів. Регулярні аудити, оцінки ризиків та впровадження нових рішень, зокрема в області штучного інтелекту, дозволять забезпечити проактивний підхід до захисту даних.

Отже, з огляду на зростаючу залежність суспільства від цифрових технологій, важливо, щоб держави, підприємства та користувачі об'єднали зусилля для створення безпечного цифрового середовища. Лише спільними зусиллями можна забезпечити надійний захист інформації, що є основою для розвитку сучасних економік і суспільств у цілому. В умовах швидко змінюваного цифрового світу забезпечення кібербезпеки має стати пріоритетом для всіх.

Інформаційні джерела:

1. Легомінова С., Гайдур Г. Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм. *Кібербезпека: освіта, наука, техніка*. 2023. № 2(22), С. 54-67. URL://doi.org/10.28925/2663-4023.2023.22.5467.

2. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ: ДУТ, 2015. 288 с.

КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СЕРВІСІВ УПРАВЛІННЯ ПІДПРИЄМСТВОМ

Кащена Н.Б., д-р екон. наук, проф.
Бакаляр Д.Г., PhD
Державний біотехнологічний університет

Інформаційно-аналітичні сервіси управління підприємством формують інформаційній простір прийняття бізнес-рішень. За умов високої невизначеності та конкуренції вони є драйверами сучасного менеджменту та розвитку бізнесу, що дозволяють оптимізувати інфокомунікаційні канали взаємодії суб’єктів економічних відносин і генерують релевантні масиви обліково-аналітичних даних для оцінки, контролю та оптимізації бізнес-процесів, підтримки інновацій та адаптації до цифрових змін, оперативного управління, стратегічного планування та прогнозування фінансово-економічних показників й ринкових трендів [1].

Інформація у сучасному світі є одним з найцінніших активів [2], а можливість оперативно її обробляти та аналізувати [3; 4] формує конкурентні переваги підприємства. Тому необхідно дбати про надійний захист обліково-аналітичних даних інформаційних сервісів. Бо їх уразливість ставить під загрозу не тільки бізнес-процеси, але й стратегічні цілі розвитку бізнесу. Так, можливі кіберзагрози (рис. 1) та компрометація даних можуть призвести до втрати конкурентних переваг, фінансових збитків і репутаційних ризиків.

Рис. 1. Кіберзагрози інформаційно-аналітичних сервісів управління підприємством

Це підкреслює важливість інтегрованої кібербезпеки, яка ґрунтується на основних принципах захисту даних (конфіденційність, цілісність, доступність), та охоплює всі рівні доступу до інформації, її шифрування, контроль прав доступу, регулярне оновлення систем і підвищення обізнаності персоналу (рис. 2).

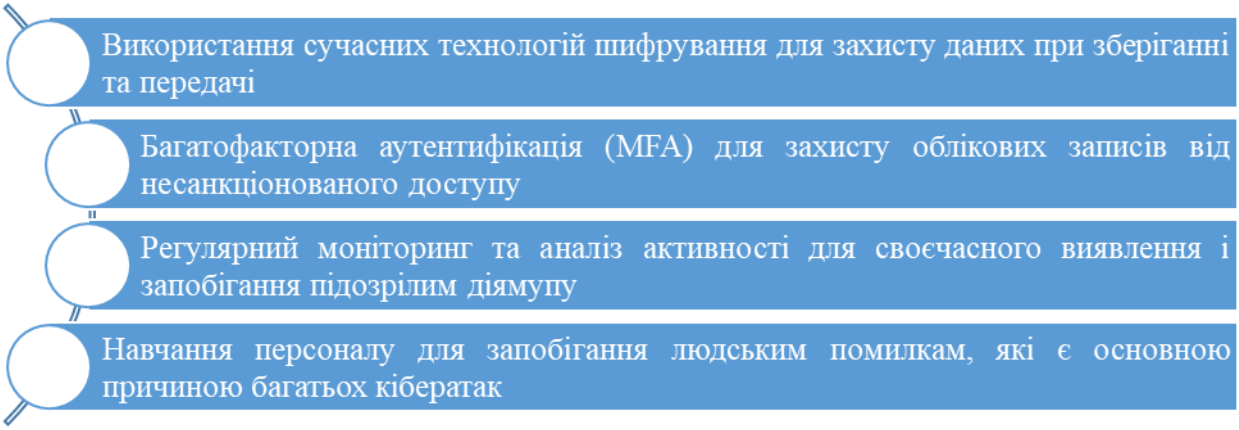

Рис. 2. Пакет заходів щодо захисту інформаційно-аналітичних сервісів

Рівень кібербезпеки інформаційно-аналітичних сервісів управління бізнесом здебільшого визначається сучасними технологіями шифрування даних (асиметричне, симетричне, протоколи TLS і IPSec, End-to-end шифрування (E2EE) тощо), які допомагають захистити фінансову інформацію підприємства від несанкціонованого доступу. Вони працюють як «ключі», що перетворюють дані в код, який можуть розшифрувати тільки уповноважені особи з правильним доступом. Так, при збереженні або надсиланні електронною

поштою фінансових звітів, шифрування захищає їх від сторонніх очей. Асиметричне шифрування використовує пару ключів: один для шифрування (публічний) і інший для розшифрування (приватний). Це дозволяє безпечно передавати конфіденційну інформацію, наприклад, про платежі. Симетричне шифрування, як-от AES, часто використовується для захисту даних в облікових системах, оскільки воно швидке й надійне. Протоколи TLS і IPSec забезпечують захист фінансової інформації при роботі в хмарних сервісах або при здійсненні онлайн-платежів. Месенджери з end-to-end шифруванням також захищають обговорення фінансових питань від перехоплення. Навіть якщо сервери зламали, зашифровані дані залишаються недоступними без ключів. Завдяки шифруванню є впевненість, що дані підприємства та бухгалтерська інформація захищені від кібератак і крадіжок.

Не менш важливою є і багатофакторна аутентифікація (MFA). Це метод додаткового захисту облікових записів, який вимагає більше ніж одного способу підтвердження особи під час входу. Зазвичай MFA поєднує щонайменше два з трьох факторів: щось, що користувач знає (пароль), щось, що він має (наприклад, телефон для отримання коду) і щось, чим він є (біометричні дані, такі як відбиток пальця). Це значно підвищує рівень безпеки, оскільки зловмисник не зможе отримати доступ до облікового запису лише з паролем. Цей метод популярний серед банків, корпоративних мереж і хмарних сервісів, де конфіденційність даних є критично важливою. Використання MFA дозволяє захистити облікові записи від несанкціонованого доступу та знижує ризик зламу.

Також є важливими заходами для забезпечення безпеки, які дозволяють вчасно виявляти та запобігати підозрілим діям в управлінських інформаційних сервісах, є регулярний моніторинг і аналіз активності. Їх реалізація забезпечує відстеження дій користувачів та процесів задля того, щоб виявити аномалії, зокрема такі як, несанкціоновані спроби доступу або незвичні зміни в даних. Це допомагає швидко реагувати на потенційні загрози й обмежити шкоду від можливих атак. Впровадження такого моніторингу сприяє не тільки захисту даних, а й формуванню безпечного середовища для користувачів і систем. У результаті ризики витоків інформації та кіберзагроз значно знижуються, забезпечуючи надійну роботу бізнесу.

І на особливу увагу заслуговує навчання персоналу з кібербезпеки. Воно є важливим кроком для зниження ризику людських помилок, які часто стають причиною кібератак. Регулярне інформування працівників про фішинг, соціальну інженерію та безпечне використання паролів допомагає уникати помилок, які можуть призвести до витоку даних. Працівники, які знають, як розпізнати підозрілі повідомлення та сайти, з меншою ймовірністю стануть жертвами обману. Навчання сприяє формуванню культури безпеки на підприємстві, де кожен розуміє свою роль у захисті даних. У результаті, підвищується загальний рівень захищеності від кіберзагроз.

Викладене доводить, що інформаційно-аналітичні сервіси управління підприємством працюють з великим обсягом чутливих даних, зокрема таких як фінансова інформація, конфіденційні дані клієнтів, внутрішні звіти та прогнози, і це робить їх особливо вразливими до кіберзагроз та актуалізує проблематику

захисту інформаційних активів. Інтегроване забезпечення безпеки цих сервісів дозволяє захистити підприємство від втрат і продовжувати ефективно використовувати їх для стратегічного розвитку в умовах сучасних викликів і динамічних змін цифрового бізнес-середовища.

Інформаційні джерела

1. Кирильєва Л., Поливана Л., Кащена Н., Наумова Т. Акімова Н. Організаційні аспекти формування інформаційно-аналітичного сервісу управління підприємствами торгівлі в період цифровізації. *Financial and Credit Activity Problems of Theory and Practice*. 2023. 3(50). 127–138. DOI: https://doi.org/10.55643/fcaptp.3.50.2023.3996

2. Kashchena N., Nesterenko I. Digitalization of the innovative development management information service of the enterprise. Mechanisms for ensuring innovative development of entrepreneurship: monograph. /Edited by T.Staverska, O.Mandych/ Tallinn: Teadmus OÜ, 2022. P.238–254. URL: https://repo.btu.kharkov.ua/bitstream/123456789/31559/1/monograph_2022_Nesterenko.pdf

3. Кащена Н. Б., Янчева Л. М. Екосистема бізнес-аналітики як мастхев інформаційно-аналітичного сервісу управління підприємствами торгівлі. *Економічна стратегія і перспективи розвитку сфери торгівлі та послуг*. 2024. Вип. 1 (35). С. 44-55. URL: https://repo.btu.kharkov.ua//handle/123456789/54668

4. Kashchena N., Nesterenko I., Chmil H., Kovalevska N., Velieva V., Lytsenko O. Digitalization of Biocluster Management on Basis of Balanced Scorecard. *Journal of Information Technology Management*, 2023. 15(4). P. 80-96. DOI: https://doi.org/10.22059/jitm.2023.94711

РОЗРОБКА ТА ДОСЛІДЖЕННЯ СИСТЕМИ АВТОМАТИЗОВАНОГО КЕРУВАННЯ СМАРТ ТЕПЛИЦЕЮ

Ковальчук Д.М., PhD
Коляка А.І., здоб. ВО
Державний біотехнологічний університет

Сьогодні, в умовах постійного зростання населення, кожна країна стикається з необхідністю вирішення питання своєчасного постачання якісних овочів та фруктів. Важливу роль у забезпеченні країни високоякісною сільськогосподарською продукцією вітчизняного виробництва відіграє ефективне функціонування тепличного господарства.

Одним із основних чинників, що гальмують розвиток тепличного господарства в Україні, є висока конкуренція на ринку. Імпортні виробники пропонують ширший асортимент овочів і ягід, які часто перевершують українську продукцію за ціною і якістю. Українські тепличні овочі не витримують конкуренції з імпортними, оскільки імпортні товари, навіть з урахуванням вартості доставки, виявляються дешевшими.

Однією з основних причин, що стримують розвиток тепличних господарств України та знижують їхню рентабельність, є високі ціни на енергоносії, які складають до 70% собівартості продукції в цьому секторі. Через це щороку відбувається скорочення площ теплиць, оскільки старі теплиці, де неможливо вирощувати продукцію з помірною собівартістю, припиняють свою