УДК 330.341
DOI:10.36919/2312-7872.1.2024.80

В. М. Бабій,
аспірант Приватного вищого навчального закладу
«Європейський університет»
e-mail: vlad.architect@gmail.com
ORCID 0009-0003-2153-6947

БЕЗПЕКОВІ АКТУАЛІТЕТИ СПЕЦІАЛІЗОВАНИХ ПРОГРАМ В УПРАВЛІННІ ПІДПРИЄМСТВОМ

Анотація. *Нинішній час відзначається збільшенням використання спеціалізованих програм для управління підприємствами. При цьому, безпека даних та інформації є однією з найбільш критичних проблем, яка потребує вирішення. У цій науковій статті досліджується питання забезпечення безпеки в спеціалізованих програмах для управління всередині підприємств. Для досягнення цієї мети було проведено аналіз поточного стану безпеки в спеціалізованих програмах та виявлено проблеми, що виникають при їх використанні. У статті описано методи та підходи до забезпечення безпеки в програмах управління підприємствами, включаючи шифрування даних, контроль доступу, аудит безпеки та захист від вірусів. Крім того, розглянуто питання безпеки в хмарних сервісах та можливі підходи до їх захисту. У результаті дослідження було встановлено, що забезпечення безпеки в спеціалізованих програмах для управління підприємствами є складним завданням, яке потребує комплексного підходу. Розроблено низку рекомендацій та рекомендованих практик, що сприятимуть покращенню рівня безпеки в програмах управління підприємствами.*

Ключові слова: *безпека інформації, програми управління підприємствами, контроль доступу, шифрування даних, аудит безпеки, захист від вірусів, хмарні сервіси, комплексний підхід, забезпечення безпеки.*

Постановка проблеми. У сучасному світі, коли все більше підприємств переходять на використання спеціалізованих програм для управління, проблема безпеки даних та інформації стає все більш актуальною. Ці спеціалізовані програми для управління підприємствами містять значну кількість конфіденційної інформації про підприємство, його клієнтів, постачальників та працівників. Як наслідок, захист цієї інформації від несанкціонованого доступу та зловмисних атак є критично важливим завданням.

Проте, існує ряд проблем, які виникають під час використання спеціалізованих програм для управління підприємствами, які можуть впливати на їх безпеку. Деякі з цих проблем включають в себе недостатній рівень захисту даних, недостатній контроль доступу, вразливості в програмному забезпеченні, недостатній аудит безпеки та недостатній захист від вірусів. Крім того, зростає популярність хмарних сервісів, які можуть створювати додаткові ризики для безпеки даних. Отже, постановка проблеми полягає у необхідності вирішення питання забезпечення безпеки в спеціалізованих програмах для управління підприємствами. Для цього необхідно виявити проблеми, що виникають під час їх використання та розробити комплексний підхід до забезпечення безпеки даних та інформації в цих програмах.

Аналіз останніх досліджень і публікацій. Останні дослідження та публікації з проблеми безпеки в спеціалізованих програмах для управління підприємствами підкреслюють критичне значення цього питання та необхідність комплексного підходу до забезпечення безпеки даних та інформації в цих програмах.

Проблематику аналізу ризиків поділити на дві групи: до першої належить розроблення наукових методів аналізу ризиків на основі відомих теорій та вимог стандартів щодо створення системи управління інформаційної безпеки; друга група містить спеціалізовані програмні продукти, які, зазвичай базуються на методах першої групи, але мають більшу практичну спрямованість і краще враховують специфіку об'єкта захисту.

Одним з авторів, який займається цією проблематикою, є Хосана Твіномурінзі з Університету Йоганнесбургу. В його статті "Mobile Cloud Based Enterprise Resource Planning Systems for Small Medium and Micro Enterprises: A Systematic Literature Review" автор провів аналіз огляд 35 рецензованих журналів і матеріалів конференцій з проблеми безпеки та приватності в системах планування ресурсів підприємства [1]. У своїй роботі він виявив, що недостатня увага до захисту

даних в системах ERP може призвести до кібератак, що загрожують безпеці та інтегритету даних підприємства.

Інший вчений, який вивчає проблему безпеки в програмах для управління підприємствами — це Тадіва Еліша Нямасвісва з Університету інфраструктури Куала-Лумпур. В його статті "A Review of Cloud-based ERP in Security Perspective" автор провів дослідження різних директив та рекомендацій щодо управління інформаційною безпекою в системах ERP [2]. Він зробив висновок, що директиви та рекомендації щодо безпеки даних повинні бути побудовані на основі комплексного підходу, що враховує ризики та загрози, які стикається підприємство. У дослідженні "Moving ERP Systems to the Cloud — Data Security Issues" Серхіо Лухан-Мора з Університету Аліканте та інші розглядають проблеми безпеки в хмарних ERP системах, які здійснюються на віддалених серверах та можуть бути доступні через мережу Інтернет [3]. Він підкреслює, що переваги, які пропонують хмарні ERP системи, такі як зменшення витрат та підвищення мобільності, також можуть виявитись джерелом загроз для безпеки даних. Автор зазначає, що хмарні ERP системи можуть бути вразливими до кібератак через використання спільного зберігання даних, зменшення контролю за фізичною інфраструктурою та несанкціонований доступ до хмарних ресурсів.

Однак, Серхіо Лухан-Мора також вказує на те, що хмарні ERP системи можуть бути безпечними, якщо будуть застосовані відповідні заходи безпеки. В своєму дослідженні автор також надає рекомендації щодо безпеки даних у хмарних ERP системах. Зокрема, він рекомендує застосування шифрування даних, двофакторної автентифікації та моніторингу безпеки. Він також радить звернути увагу на вибір хмарного провайдера та вимоги до його безпеки. У своєму дослідженні Серхіо Лухан-Мора підкреслює необхідність розглядати проблему безпеки в контексті конкретного підприємства та його потреб. Він вважає, що безпека даних має бути вбудована в дизайн системи та має бути постійно оновлювана та адаптована до змін в інформаційному середовищі підприємства.

Метою дослідження є дослідження питання забезпечення безпеки в спеціалізованих програмах для управління всередині підприємств з метою виявлення можливих загроз, що виникають при використанні таких програм, а також розробка рекомендацій щодо покращення безпеки використання таких програм на підприємствах. Для досягнення цієї мети розглядаються основні проблеми та виклики, що виникають при забезпеченні безпеки в програмах управління підприємствами, а також вивчаються основні методи та підходи до забезпечення безпеки в таких програмах.

Виклад основного матеріалу дослідження. В наші часи без ефективних програмних систем збереження даних не обійдеться практично жодне підприємство. Це можуть бути різного роду підприємства: банки, страхові, транспортні компанії, мережі супермаркетів, телекомунікаційні та маркетингові фірми, організації, що задіяні в сферах послуг тощо [4, 5]. Дослідження починається з аналізу останніх досліджень та публікацій з даної тематики, де виявлено, що існує багато проблем та викликів, пов'язаних з забезпеченням безпеки в програмах управління підприємствами [6, 7, 8]. Сховище даних — це організований масив даних підприємства, що обробляється і зберігається в єдиному апаратно-програмному комплексі, що забезпечує швидкий доступ до даних підприємства, багатовимірний аналіз даних, створення звітів з метою відображення статистичних даних [9].

Зокрема, серед проблем можна виділити недостатню увагу до безпеки в програмах, неефективне використання засобів захисту, недостатню компетентність персоналу тощо. У дослідженні також розглядаються основні методи та підходи до забезпечення безпеки в програмах управління підприємствами. Наприклад, вихідні дані можуть бути агреговані протягом певного періоду часу шляхом застосування статистичних функцій над даними, такими як визначення середнього арифметичного, максимального або мінімального значення, суми значень, підрахунок кількості значень. Після виконання процедури агрегування даних вони можуть бути представлені засобами формування звітів з метою прийняття бізнес-рішень.

Серед основних завдань є розробка та впровадження спеціальних механізмів захисту інформації, які забезпечують захист від вторгнень та злому та використання криптографічних алгоритмів та методів шифрування для захисту конфіденційної інформації. Також важливо проведення аудиту програмного забезпечення та пошуку потенційних вразливостей у системах управління [10].

На першому етапі роботи алгоритму розраховують рівень загрози за вразливістю *Th* на основі критичності та ймовірності реалізації загрози менеджменту підприємству через цю вразливість [11]. Рівень загрози передбачає, наскільки критичним є вплив цієї загрози на базу з врахуванням ймовірності її реалізації.

$$Th - \frac{ER}{100} * \frac{P(V)}{100}, \quad (1)$$

де *ER* — критичність появи загрози *(у %)*, *P(V)* — ймовірність появи загрози менеджменту підприємству через цю вразливість *(у %)*, *Th* — рівень загрози за вразливістю.

Другий етап передбачає розрахунок рівня загроз менеджменту підприємству за всіма вразливостями *CTh* , через які можлива нетралізувати цю загрозу на підприємстві. Підсумуємо отримані рівні загроз через конкретні вразливості менеджменту підприємству за такоюформулою:

$$CTh = 1 - \prod_{i=1}^{n}(1 - Th_i), \quad (2)$$

де *CTh* — рівень загрози менеджменту підприємству за всіма вразливостями, *Th* — рівень загрози менеджменту підприємству за вразливістю. Значення рівня загрози менеджменту підприємству за всіма вразливостями має знаходитись у межах від 0 до1.

На третьму етапі аналогічно розраховуємо загальний рівень загроз менеджменту підприємству за доступом до інформації *CThR* (враховуючи всі загрози менеджменту підприємству

$$CThR = 1 - \prod_{i=1}^{n}(1 - CTh_i), \quad (3)$$

де *CThR* — загальний рівень загроз менеджменту підприємству, *CTh* — рівень загрози менеджменту підприємству за всіма вразливостями.

На четвертому етапі ризик за доступом *R* розраховують так:

$$R = CTh * D, \quad (4)$$

де *R* — ризик за доступом, *CThR* — загальний рівень загроз менеджменту підприємству за доступом, *D* — критичність доступу.

Критичність доступу визначають за такою формулою:

$$D = D_t * T, \quad (5)$$

де D_t – критичність доступу за загрозою менеджменту підприємству доступності, *T* — максимально критичний час простою доступу.

На п`ятому етапі ризик за ІС *CR* розраховують за формулою:

$$CR = \left(1 - \prod_{i=1}^{n}\left(1 - \frac{R_i}{100}\right)\right) * 100, \quad (6)$$

де CR — ризик за ІС, R — ризик за доступом.

Основні функції апаратних засобів захисту:

– заборона несанкціонованого (неавторизованого) внутрішнього доступу до баз даних в результаті випадкових чи умисних дій персоналу;

– заборона несанкціонованого (неавторизованого) зовнішнього доступу віддаленого користувача до ресурсів локальної мережі;

– захист цілісності програмного забезпечення.

До апаратних засобів захисту даних від їх пошкодження належать:

1) джерела безперебійного живлення апаратури;

2) пристрої стабілізації напруги;

3) пристрої екранування апаратури, ліній зв'язку та приміщень.

До апаратних засобів захисту від несанкціонованого доступу належать:

1) пристрої захисту портів комп'ютерної техніки;

2) засоби блокування пристроїв та інтерфейсів введення/виведення;

3) апаратні ключі (призначені для захисту програмного забезпечення і даних від копіювання, нелегального використання і несанкціонованого розповсюдження);

4) електронні замки (виконують контроль завантаження комп'ютера і перевіряють цілісність операційної системи).

До програмно-апаратних пристроїв захисту належать:

1) засоби резервування та архівування даних, що дозволяють повернути стан системи на момент її резервування;

2) пристрої ідентифікації та фіксації терміналів і користувачів при спробах несанкціонованого доступу до комп'ютерної мережі;

3) Е-токени (OTP-токени, смарт-карти, смарт-карти з генератором одноразових паролів, ActiveCard, USB-ключі, USB-ключі з генераторами одноразових паролів). Е-токени найбільш поширені в автоматизованих банківських системах.

4) апаратні шифратори (плати розширення, що вставляються в роз'єми системної плати ПК або виготовляються у вигляді USB-ключа з криптографічними функціями);

5) криптографічні плати, за допомогою яких можна зашифрувати дані та накласти електронний цифровий підпис (ЕЦП) на електронний документ.

OTP-токени використовуються для генерації шестизначних одноразових паролів. Пароль змінюється кожні 60 секунд і призначений для аутентифікації власника з метою його доступу до віддалених інформаційних ресурсів. Цей прилад не є сховищем ключів, він автономний (не прив'язаний до комп'ютера власника). Кожен OTP-токен має унікальний серійний номер. Смарт-карти — це магнітні карти для зберігання таємних ключів, накладання ЕЦП та шифрування паролів доступу. Для смарт-карти потрібен спеціальний зчитувач карток, який повинен завжди бути з користувачем [12].

У смарт-картах з генератором одноразових паролів останній формується на чіпі смарт-карти. E-Token з функціями смарт-карти має недолік: PIN-код вводиться не з власної клавіатури пристрою, а з клавіатури терміналу, до якого пристрій підключений. Одноразовий пароль (OTP) дійсний тільки для одного сеансу аутентифікації, його дія також може бути обмежена певним проміжком часу.

Перевага такого паролю порівняно зі статичним полягає в тому, що його не можна використовувати повторно (зловмисник, що перехопивши дані з успішної сесії автентифікації, не може використовувати скопійований пароль для отримання доступу до захищеної інформаційної системи). Алгоритми створення OTP зазвичай використовують випадкові числа, щоб не можна було передбачити подальші паролі на основі знання попередніх. Одноразові паролі можуть генеруватися банком — в цьому випадку користувач має можливість отримувати їх різними способами: в банкоматі, як SMS-повідомлення (в Україні найпоширеніший нині спосіб), як список (TAN-коди) тощо. Одноразові паролі також можуть генеруватися і на боці клієнта з використанням автономних генераторів одноразових паролів (токенів) або рішень, інтегрованих у смарт- карти останнього покоління.

ActiveCard — це пристрій для введення паролю доступу (динамічного оду), який розраховується [13].

Всередині ActiveCard вмонтований мікропроцесор, у пам'яті якого зберігається секретний код. Чотиризначний пароль, що водиться користувачем, перераховується, тобто створюється спеціальний код. Для зчитування паролю потрібен SmartReader. USB-ключі (апаратні токени) призначені для захищеного зберігання і використання ключів ЕЦП: формування і перевірки ЕЦП, шифрування, автентифікації, зберігання ключової інформації.

Для апаратного токена потрібен USB-порт. USB-ключі з генераторами одноразових паролів можна використовувати і без USB-порта, тобто в поєднанні з такими пристроями, як смартфони або планшети. За допомогою USB-ключа можна захистити обліковий запис на комп'ютері, використовуючи складний пароль, який не треба запам'ятовувати.

Для цього потрібне програмне забезпечення і USB-ключ, який для нього підходить. За допомогою програми USB отримає ключ для входження в систему. При повторному завантаженні слід вставити апаратний ключ (наприклад, в USB- порт) і ввести PIN-код.

Використовувати цілу плату тільки для функцій шифрування недоцільно з точки зору економічних показників, тому виробники зазвичай намагаються дооснастити їх різними додатковими можливостями, серед яких є такі:

1) Контроль завантаження комп'ютера. При його включенні пристрій вимагає від користувача ввести персональну інформацію (наприклад, вставити дискету з ключами). Робота буде дозволена тільки після того, як пристрій розпізнає пред'явлені ключі і вважатиме їх «своїми». В іншому випадку доведеться вилучати шифратор, щоб завантажити комп'ютер. Проте, інформація на ПК теж має підлягати шифруванню.

2) Контроль цілісності файлів операційної системи. Використання цього підходу не дозволить зловмиснику змінити які-небудь дані. Шифратор зберігає в собі список всіх важливих файлів із заздалегідь розрахованими для кожного з них контрольними сумами (або хеш-значеннями). І якщо при наступному завантаженні не співпаде еталонна сума хоча б з одним з них, комп'ютер буде блокований.

3) Генерація випадкових чисел для отримання криптографічних ключів та ЕЦП. При кожному обчисленні підпису використовується випадкове число. Плата з усіма перерахованими можливостями називається пристроєм криптографічного захисту даних. Токени можуть підключатися до комп'ютера і з використанням безпровідникових технологій (RFID).

Такі токени передають ключову послідовність локальному клієнту або до найближчої точки доступу без фізичного підключення. Bluetooth-токени можуть працювати в поєднанні з мобільними пристроями. Bluetooh-токенам потрібний власний елемент живлення, тому в них вмонтовується акумулятор, який періодично потрібно заряджати (час безперебійної роботи близько 40 годин). Bluetooth- аутентифікація працює на відстані до 10 метрів.

Безпровідникові токени мають відносно невеликий термін придатності — 3–5 років. У їх якості можуть використовуватись також мобільні пристрої — смартфони та планшети. Вони також можуть забезпечувати аутентифікацію, в тому числі з використанням криптографічних ключів.

Таким чином, на першому місці на підприємстві стоїть завдання розробки системи моніторингу безпеки, яка буде надавати оперативну інформацію про потенційні загрози безпеці в режимі реального часу. Використання системи аутентифікації та авторизації, яка дозволяє контролювати доступ до конфіденційної інформації та забезпечити її захист від несанкціонованого доступу. Розробка та впровадження процедур резервного копіювання, які дозволяють відновлювати інформацію у випадку її втрати або пошкодження. Використання систем виявлення та усунення вразливостей, які дозволять автоматично виявляти і усувати потенційні загрози безпеці.

Висновки з проведеного дослідження. Безпека є надзвичайно важливим аспектом для підприємств, які використовують спеціалізовані програми для управління, оскільки недостатня захист може призвести до витоку конфіденційної інформації, порушення правил регулювання і втрати довіри клієнтів. Для забезпечення безпеки в програмах управління необхідно використовувати комплексний підхід, який включає в себе технічні та організаційні заходи. Важливість внутрішнього контролю та моніторингу системи безпеки не може бути переоцінена, оскільки це дозволяє вчасно виявляти та запобігати можливим загрозам. Незважаючи на наявність різноманітних засобів захисту, необхідно зберігати свідомість про можливі загрози та змінювати підходи до захисту відповідно до зміни умов та технологій.

Апаратно-програмні засоби захисту використовуються для аутентифікації користувачів в корпоративних локальних мережах, автоматизованих банківських системах, апаратурі шифрування в системі електронних платежів НБУ, апаратурі накладання ЕЦП відповідальних осіб на електронні документи та його перевірці.

Дослідження показали, що розробка та впровадження ефективних заходів безпеки в програмах управління підприємством може знизити ризик витоку конфіденційної інформації та збільшити довіру клієнтів та стейкхолдерів. Отже, безпека в спеціалізованих програмах для управління всередині підприємства є надзвичайно важливим аспектом, який вимагає комплексного підходу та постійного контролю, щоб забезпечити захист конфіденційної інформації та довіру.

REFERENCES

1. Twinomurinzi H. (2023) / Mobile Cloud Based Enterprise Resource Planning Systems for Small Medium and Micro Enterprises: A Systematic Literature Review. Digital-for-Development: Enabling Transformation, Inclusion and Sustainability Through ICTs Vol. 1774 P. 46–69.

2. Nyamasvisva T.E. A (2022) / Review of Cloud-based ERP in Security Perspective. International Journal of Engineering Research and Applications.. Vol. 12(8) P. 66–70.

3. Luján-Mora S., Costales A, Moscoso-Zea O. and Saa P. Moving ERP (2017) / Systems to the Cloud — Data Security Issues. Journal of Information Systems Engineering & Management. Vol. 2(4) P. 21–29.

4. Amladi P. (2017)/ HR's guide to the digital transformation: ten digital economy use cases for trans-forming human resources in manufacturing. Strategic HR Review, vol. 16 (2), pp. 66–70.

5. Bondarouk T. and H.J.M. Ruel (2010)/ Electronic human resource management: challenges in the digi-tal era. International Journal of Human Resource Management, vol. 20 (3), pp. 505–514.

6. Calvard T.S. and D. Jeske (2018) / Developing human resource data risk management in the age of bigdata. International Journal of Information Management, vol. 43, pp. 159–164.

7. Marler J.H. and J.W. Boudreau (2017) / An evidence-based review of HR Analytics. International Journal of Human Resource Management, vol. 28 (1), pp. 3–26.

8. Marler J.H., S.L. Fisher and W. Ke (2010)/ Employee self-service technology acceptance: A comparisonof pre-implementation and post-implementation relationships. Personnel Psychology, vol. 62 (2), pp. 327–358.

9. Neeraj (2018)/ Role of digitalization in human resource management. International Journal of Emerging Technologies and Innovative Research, vol. 5 (1), pp. 284–288. Available at: http://www. jetir.org/ papers/JETIR1801055.pdf

10. Panayotopoulou L., E. Galanaki and N. Papalexandris (2010)/ Adoption of electronic systems inHRM: is national background of the firm relevant? New Technology, Work and Employment, vol. 25 (3), pp. 253–269.

11. Parry E. and S. Tyson (2011) / Desired goals and actual outcomes of E-HRM. Human Resource Management Journal, vol. 21 (3), pp. 335–354.

12. Quaosar G.A.A. (2017) / Determinants of the adoption of human resources information systems in adeveloping country: an empirical study. International Technology Management Review, vol. 6 (3), pp. 82–93.

13. Ruel H. and H. Van der Kaap (2012)/ E-HRM usage and value creation. Does a facilitating contextmatter? German Journal of Human Resource Management, vol. 26 (3), pp. 260–281.

V. M. Babii. ENSURING SECURITY OF SPECIALIZED PROGRAMS IN ENTERPRISE MANAGEMENT

Abstract. *The current time is marked by an increase in the use of specialized programs for enterprise management. At the same time, the security of data and information is one of the most critical problems that needs to be solved. This scientific article examines the issue of ensuring security in specialized programs for management within enterprises. To achieve this goal, an analysis of the current state of security in specialized programs was carried out and problems that arise when using them were identified. The article describes methods and approaches to ensure security in enterprise management applications, including data encryption, access control, security auditing, and virus protection. In addition, the issue of security in cloud services and possible approaches to their protection are considered. As a result of the study, it was established that ensuring security in specialized programs for enterprise management is a complex task that requires a comprehensive approach. A number of recommendations and recommended practices have been developed that will contribute to improving the level of security in enterprise management programs.*

Keywords: *information security, enterprise management programs, access control; data encryption, security audit, protection against viruses, cloud services, integrated approach, security practices.*