Ключевые слова: контроль технического состояния, встроенные вычислительные системы, техническая диагностика.

Keywords: technical control, embedded system, technical diagnostics.

Логінова Наталія Іванівна

Національний університет «Одеська юридична академія»

завідуюча кафедрою інформаційних технологій,

кандидат педагогічних наук, доцент

БЕЗПЕКА БАЗ ДАНИХ

Цифрова трансформація всіх сфер життєдіяльності призвела до того, що за допомогою інформаційно-комунікаційних технологій стало можливим зберігати, передавати та обробляти величезні масиви даних. Без використання таких масивів в електронному вигляді сьогодні не обходиться жодна організація чи підприємство, незалежно від форми власності. При цьому в сучасних інформаційних системах циркулюють різні типи даних, зокрема конфіденційні. Це створює передумови для здійснення різних неправомірних діянь та кіберзлочинів, зокрема, несанкціонованого доступу до інформації, крадіжки персональних даних, модифікації або знищення їх. Цінність такої інформації й сприяє підвищенню безпеки інформаційної системи, у тому числі й баз даних, які є основними елементами таких систем.

Головне завдання будь-якої бази даних – збереження величезних масивів даних, які повинні зберігатися з гарантуванням безпеки та конфіденційності.

Захист баз даних є одним із складних завдань у сфері інформаційної безпеки, оскільки не існує однакових баз даних. Вони відрізняються структурою побудови, способами обробки та доступу до даних, прикладними системами та багатьом іншим. Тому для кожної бази даних необхідно використовувати індивідуальний підхід до організації захисту та забезпечення безпеки.

Захист баз даних включає велику кількість технологій та інструментів, які дозволяють забезпечити безпеку збережених даних і захистити системи керування базами даних [1]. Найбільш ефективними заходами в цій сфері є:

- розподіл ресурсів баз даних та серверів;
- шифрування файлів та резервних копій баз даних;
- оновлення програмного забезпечення;
- здійснення контролю безпеки доступу до бази даних;
- аудит та моніторинг активності бази даних.

Численні інциденти хакерських атак показують, що найбільш уразливими є сервери, розміщені в «хмарах» і на різних зовнішніх хостингах. Розподіл ресурсів бази даних та серверів є надійним способом захисту даних. Наприклад, згідно з п. 2.2.1 Стандарту безпеки даних платіжних карток PCI-DSS (Payment Card Industry Data Security Standard) будь-яка база даних, що містить конфіденційну інформацію, повинна зберігатися на сервері, який безпосередньо не взаємодіє з Інтернетом [2].

Шифрування даних є стандартною процедурою багатьох баз даних. Але для захисту необхідно регулярно створювати резервні копії бази даних, які повинні бути зашифровані та зберігатися окремо від ключів дешифрування. Резервне копіювання бази даних захищає не тільки від атак хакерів, але і від збоїв, які можуть статися з обладнанням та програмним забезпеченням.

Оновлення програмного забезпечення бази даних має відбуватися регулярно. Необхідно встановлювати всі виправлення безпеки та захисту від вразливостей інформаційної системи, що постійно виявляються. Потрібно використовувати елементи керування безпеки, що надаються базою даних. Це особливо важливо для баз даних, підключених до великої кількості сторонніх застосунків, кожний з яких потребує виправлення.

Безпечний доступ до бази даних є одним із способів захисту. Необхідно прагнути мінімальної кількості користувачів, які мають доступ до ресурсів. Користувачам треба надавати мінімальні привілеї, що необхідні для виконання роботи з використанням бази даних, і лише у певний період. Потрібно керувати дозволами за допомогою груп та розмежувати ролі, а не надавати прямий доступ.

Рекомендується застосовувати автоматизоване керування доступом за допомогою спеціального програмного забезпечення. Це дозволить користувачам надавати тимчасовий пароль, який буде генеруватиметься при кожному вході до бази даних. При цьому щоразу надаватимуться тільки ті права, які їм необхідні в даний момент при роботі з базою даних. Це також дозволить відстежувати всі дії, виконані цим користувачем. Для захисту бази даних необхідно налаштувати стандартні процедури безпеки облікових записів. Користувачі повинні використовувати надійні паролі, хеш яких повинні зберігатися в зашифрованому вигляді. Необхідно налаштувати блокування записів користувачів після мінімальної кількості спроб входу до бази даних.

Моніторинг спроб входу до бази даних дозволяє визначити аномальні активності та зламування облікових записів. Моніторинг відбувається аналізом трафіку протоколу, який здійснюється від сервера управління мережею. За допомогою програмних агентів, які розміщуються на сервері керування можна налаштувати спостереження за активністю локальної бази даних на окремому сервері бази даних. Аудит працездатності бази даних дозволяє виявити системні проблеми та порушення політики конфіденційності та витоків даних, зіставляти дії у базі даних із подіями безпеки, створювати журнали аудиту всіх дій у базі даних.

Отже, для запобігання витоку інформації необхідно реалізувати комплексний захист бази даних. Необхідно використовувати розподіл доступу користувачів, розподілені ресурси баз даних та серверів, проводити моніторинг дій користувачів та аудит працездатності бази даних. Використовувати засоби шифрування файлів та резервних копій. Всі ці заходи необхідні для мінімізації ризиків, пов’язаних з втратою конфіденційної інформації баз даних і захисту інформаційної системи.

Список використаних джерел:

1. Database Security: 7 Best Practices & Tips. URL: https://www.esecurityplanet.com/networks/database-security-best-practices/ (дата звернення: 01.11.2021)

2. Is Splitting off Resources for Your Database Right for You? URL: https://www.liquidweb.com/blog/is-splitting-off-resources-for-your-database-right-for-you/ (дата звернення: 01.11.2021)

Ключові слова: база даних, захист даних, безпека баз даних, ресурси баз даних, інформаційна система

Ключевые слова: база данных, защита данных, безопасность баз данных, ресурсы баз данных, информационная система

Keywords: database, data protection, database security, database resources, information system

Василенко Микола Дмитрович

Національний університет «Одеська юридична академія», професор кафедри кібербезпеки, доктор фізико-математичних наук, доктор юридичних наук, професор

Шевченко Тетяна Вікторівна

Державний університет «Одеська політехніка», доцент кафедри міжнародних відносин та права, кандидат юридичних наук

ШТУЧНИЙ ІНТЕЛЕКТ ТА ЙОГО БЕЗПЕКА В ПУБЛІЧНОМУ АДМІНІСТРУВАННІ

Темпи розвитку штучного інтелекту (ШІ) дозволяють говорити про його суттєве використання в публічному адмініструванні. В Україні на виконавчому рівні задекларовано впровадження ШІ (високого порядку) в публічне управління і не тільки [1]. Однак ШІ такого порядку потребує відповідних інтелектуальних систем захисту інформації. Вони передбачають інтелектуалізації цих систем. При цьому все ж таки залишається відсутнім належне обґрунтування наслідків самих заходів щодо застосування ШІ в адміністративному управлінні щодо