# СЕКЦІЯ 12

# ІНФОРМАТИЗАЦІЯ СУСПІЛЬСТВА ТА ЗАХИСТ ІНФОРМАЦІЇ В УМОВАХ ВІЙСЬКОВОГО ВТОРГНЕННЯ

***Керівник секції:*** *завідувач кафедри інформаційних технологій, кандидат педагогічних наук, доцент Н. І. Логінова*

***Секретар секції:*** *асистент кафедри інформаційних технологій А. А. Толокнов*

***ЛОГІНОВА НАТАЛІЯ ІВАНІВНА***

*Національний університет «Одеська юридична академія», завідувач кафедри інформаційних технологій, кандидат педагогічних наук, доцент*

***ДИКА АНАСТАСІЯ ІВАНІВНА***

*Національний університет «Одеська юридична академія», асистент кафедри інформаційних технологій*

***ЯНКОВСЬКИЙ ОЛЕГ ГЕОРГІЙОВИЧ***

*Національний університет «Одеська юридична академія», доцент кафедри інформаційних технологій, кандидат технічних наук, доцент*

## АНАЛІЗ ВРАЗЛИВОСТЕЙ СИСТЕМ КЕРУВАННЯ БАЗАМИ ДАНИХ

У сучасному світі цифрового панування дані є головним ресурсом людини, компанії, організації тощо. Для керування великими масивами даних використовують сервера з системами керування базами даних (СКБД).

СКБД – це комплекс мовних і програмних засобів, призначений для створення, ведення і сумісного використання баз даних (БД) багатьма користувачами. Основне призначення СКБД – надання користувачам БД засобів маніпулювання даними в абстрактних термінах, не пов'язаних зі способом їхнього зберігання в обчислювальній системі [1].

Нині використовуються різні СКБД – реляційні та нереляційні, які відрізняються типами зберігання даних. Кожна СКБД має свої переваги

та недоліки, тому при виборі СКБД для керування даними потрібно розуміти всі функціональні можливості системи, а також вразливості та загрози, що можуть стати причиною витоку інформації.

Аналіз вразливостей передбачає пошук загроз, вразливих місць та ризиків несанкціонованого проникнення зловмисників у СКБД. СКБД, що використовується, повинна буди захищеною та гарантувати конфіденційність, цілісність та доступність даних.

Конфіденційність даних в СКБД – це властивість, яка показує на необхідність введення обмежень на коло користувачів, які мають до цих даних доступ.

Цілісність даних в СКБД полягає у існуванні цих даних у незмінному вигляді у певний момент часу та здатність СКБД запобігати несанкціонованому доступу до даних.

Доступність даних у СКБД – це властивість, яка дозволяє системі своєчасно та безперешкодно отримувати доступ до даних користувачів, які мають відповідні права.

Безпека БД складається з використання різних процедур та функцій, які гарантують протидію загрозам та вразливостям.

Деякі з вразливостей в СКБД є діями програмних помилок, слабкими структурами, некоректного налаштування системних правил тощо, що може вплинути на безпеку системи та спровокувати зовнішні атаки, спричинені небезпечними привілеями авторизації.

У сучасних СКБД виділяють наступні вразливості [2]:

1. Підвищені привілеї: БД містять, як правило, конфіденційні дані, тому існує ризик, що користувачам будуть надані права доступу, які набагато перевершують їхні потреби у роботі з БД. Для мінімізації таких ризиків рекомендується встановлювати облікові записи з мінімальними привілеями та заблокувати можливості виконання коду з облікових записів адміністратора або власника БД.

2. Зловживання привілеями: користувачі, які мають доступ до БД, можуть за матеріальну винагороду надати стороннім особам конфіденційну інформацію або несумлінне використання інформації в БД, що може привести до її пошкодження або знищення.

3. Використання вразливостей БД для зміни прав користування від користувача з обмеженими можливостями до адміністратора. Такі вразливості можуть бути використані у процедурах, вбудованих функціях, протоколах та операторах SQL. Для запобігання таким загрозам необхідно використовувати системи запобігання вторгненням та контроль доступу на рівні запитів.

4. Впровадження SQL-ін'єкцій: сервери БД вразливі для атак, які виконуються командами запитів і дозволяють внести код зловмисників у код БД та отримати доступ до всіх даних. Для запобігання SQL-ін'єкцій необхідно сканування всіх даних БД на наявність символів, що використовуються для виконання шкідливого коду.

5. Слабка політика аудиту БД є серйозним ризиком, оскільки механізми аудиту БД дозволяють аналізувати поточний стан БД,

відстежувати дії системи та користувачів, виявляти проблемні місця в кодах програми та формувати рекомендації щодо їх усунення.

6. Відмова в обслуговуванні (DoS) – це поширений клас атак на рівні застосунків, при яких зловмисники заповнюють БД фальшивими запитами. Це знижує продуктивність роботи користувачів і може призвести до неможливості роботи систематизованих застосунків та відмови законним користувачам у доступі до БД.

7. Вразливості протоколу передачі. Будь-яке використання мережі інтернет є потенційним джерелом атак на дані, тому необхідно використовувати брандмауери для запобігання несанкціонованому доступу до БД, блокування міжсайтових сценаріїв та SQL-ін'єкцій.

8. Слабка система аутентифікації дозволяє зловмисникам видавати себе за законних користувачів шляхом отримання облікових даних для входу.

9. Низька система захисту носіїв резервного копіювання даних БД. Резервні копії БД повинні бути зашифровані та зберігатися окремо від ключів дешифрування. Таки копії БД повинні бути захищені не лише від несанкціонованого доступу, а й від збоїв апаратного та програмного забезпечення [3].

Згідно індексу TOPDB Top Database в 2022 році найбільш використовуваними СКБД є: Oracle – 32,49 %, MySQL – 16,75 %, SQL Server – 13,86 %. На ці СКБД припадає більш 63 % загальної кількості користувачів [4]. Розробники цих СКБД використовують різні інструменти для захисту даних користувачів в БД.

СКБД MySQL є стандартом для вебсерверів. У ній використовується система безпеки для всіх підключень, запитів та інших операцій, які можуть виконувати користувачі, що базується на списках контролю доступу ACL (Access Control Lists). Також забезпечується підтримка SSL-з'єднань між клієнтами та серверами MySQL.

Безпека СКБД SQL Server забезпечується за допомогою умовного доступу, аудиту та шифрування. Умовний доступ реалізується політикою ролей користувачів, що дозволяє контролювати доступом до даних БД. Для аудиту в системі використовується вбудований інструмент SQL Server Audit, який зчитує журнали транзакцій та записує інформацію про всі зміни БД. З'єднання з SQL Server можуть бути захищені за допомогою шифрування SSL/TLS.

СКБД Oracle запобігає ризикам витоку даних за допомогою різних рішень безпеки, зокрема: шифрування та управління ключами, організації контролю доступу, комплексної системи моніторингу дій та різних параметрів аудиту. Останні версії програми призначені для хмарного середовища, тому для безпеки даних всі транзакції ізольовані одна від одної.

Отже, аналіз вразливостей СКБД показав, що існують численні ризики та загрози інформації у БД. Виробники сучасних СКБД використовують комплексні механізми захисту даних, спрямовані на мінімізацію ризиків та загроз інформації користувачів БД.

***Список використаних джерел:***

1. Організація баз даних : навч. посібник / О. Г. Трофименко, Ю. В. Прокоп, Н. І. Логінова, І. М. Копитчук. 2-ге вид. виправ. і доповн. Одеса : Фенікс, 2019. С. 7-8.
2. Hassan Bediar. Challenges and Security Vulnerabilities to Impact on Database Systems. *Al-Mustansiriyah Journal of Science*. Volume 29, Issue 2, 2018. DOI: http://doi.org/10.23851/mjs.v29i2.332. URL: https://www.researchgate.net/publication/329025438_Challenges_and_Security_Vulnerabilities_to_Impact_on_Database_Systems
3. Логінова Н. І. Безпека баз даних. *Кібербезпека в сучасному світі* : матеріали ІІІ Всеукр. наук.-практич. конф. (м. Одеса, 19 листоп., 2021 р.) / за ред. О. В. Дикого; уклад.: С. А. Горбаченко, Н. І. Логінова. Одеса : Видавничий дім «Гельветика», 2021. С. 12–15. DOI 10.32837/11300.15973.
4. TOPDB Top Database index. URL: https://pypl.github.io/DB.html

**Ключові слова:** бази даних, системи керування базами даних, вразливості, безпека, загрози, ризики.

**Key words:** databases, database management systems, vulnerabilities, security, threats, risks.

***ЗАДЕРЕЙКО ОЛЕКСАНДР ВЛАДИСЛАВОВИЧ***

*Національний університет «Одеська юридична академія»,*
*доцент кафедри інформаційних технологій,*
*кандидат технічних наук, доцент*

***КУХАРЕНКО СЕРГІЙ ВІКТОРОВИЧ***

*Національний університет «Одеська юридична академія»,*
*доцент кафедри кібербезпеки, кандидат технічних наук*

## ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ВІД ВИТОКІВ В ОПЕРАЦІЙНИХ СИСТЕМАХ СІМЕЙСТВА WINDOWS

Більшість користувачів операційної системи (ОС) Windows зустрічали у списку диспетчера завдань, безліч процесів з ім'ям *svchost.exe*. Залежно від версії ОС Windows та її конфігурації, кількість таких процесів може становити від кількох одиниць до кількох десятків.

Це пояснюється тим, що *svchost.exe* є основним процесом для системних служб ОС Windows, що завантажуються з динамічних бібліотек (*.dll). Виконуваний файл *svchost.exe* розміщено у системному каталозі \Windows\system32\. Запуск системних служб організований так, що дозволяє суттєво зменшити витрати оперативної пам'яті та ресурсів процесора. Усі копії процесів ***svchost.exe*** запускаються системним процесом *services.exe* під час початкового завантаження ОС Windows, а також під час виконання системних процесів та процесів, пов'язаних