**Тема 30: Захист баз даних**

## Поняття захисту інформації

**Захист інформації** – комплекс заходів, спрямованих на забезпечення найважливіших аспектів інформаційної безпеки. На сьогоднішній день існують такі **аспекти захисту інформації**, як:

- цілісність – захист інформації від несанкціонованої модифікації;
- конфіденційність – захист від несанкціонованого ознайомлення з інформацією;
- доступність – захист (забезпечення) доступу до інформації, а також можливості її використання. Доступність забезпечується як підтриманням систем в робочому стані так і завдяки способам, які дозволяють швидко відновити втрачену чи пошкоджену інформацію.

Відповідно, до даних аспектів захисту інформації, виділяють наступні **загрози інформації:**

- загрози цілісності (знищення та модифікація інформації);
- загрози доступності (блокування та знищення інформації);
- загрози конфіденційності (несанкціонований доступ (НСД), витік та розголошення інформації).

Система називається безпечною, якщо вона, використовуючи відповідні апаратні і програмні засоби, управляє доступом до інформації так, що тільки належним чином авторизовані особи або ж діють від їхнього імені процеси отримують право читати, писати, створювати і видаляти інформацію. Очевидно, що абсолютно безпечних систем немає, і тут мова йде про надійну систему у сенсі "система, якій можна довіряти" (як, наприклад, можна довіряти людині). Система вважається надійною, якщо вона з використанням достатніх апаратних і програмних засобів забезпечує одночасну обробку інформації різного ступеня секретності групою користувачів без порушення прав доступу. Основними критеріями оцінки надійності є: - політика безпеки; - гарантованість.

Політика безпеки, будучи активним компонентом захисту (включає в себе аналіз можливих загроз і вибір відповідних заходів протидії), відображає той набір законів, правил і норм поведінки, яким користується конкретна організація при обробці, захисту та поширенні інформації. Вибір конкретних механізмів забезпечення безпеки системи здійснюється відповідно до сформульованої політики безпеки.

Гарантованість, будучи пасивним елементом захисту, відображає міру довіри, яка може бути надана архітектурі та реалізації системи (іншими словами, показує, наскільки коректно обрано механізми, що забезпечують безпеку системи).

У надійній системі повинні реєструватися всі події, що відбуваються і стосуються безпеки (повинен використовуватися механізм підзвітності протоколювання, що доповнює аналізом заповненої інформації, тобто аудитом). При оцінці ступеня гарантованості, з якою систему можна вважати надійною, центральне місце займає достовірна (надійна) обчислювальна база. Достовірна обчислювальна база (ДОБ) являє собою повну сукупність захисних механізмів комп'ютерної системи, яка

використовується для втілення в  життя відповідної політики безпеки. Надійність ДОБ залежить виключно від її реалізації та коректності введених даних (наприклад, даних про благонадійність користувачів, які визначаються адміністрацією). Кордон ДОБ утворює периметр безпеки. Компоненти ДОБ, що знаходяться всередині цього кордону, повинні бути надійними (отже, для оцінки надійності комп'ютерної системи досить розглянути тільки її ДОБ). Від компонентів, що знаходяться поза периметром безпеки не потрібно надійності. Однак це не повинно впливати на безпеку системи.

**Основні методи захисту інформації в БД**

Головним завданням бази даних (БД) є збереження значних обсягів інформації (даних). Дані в базах даних повинні зберігатися з гарантування безпеки та конфіденційності. Інформація не повинна бути загубленою або викраденої. Загрози втрати конфіденційної інформації стали звичайним явищем у сучасному комп’ютерному світі.

**Якщо в системі захисту є недоліки, то даним може бути завдано шкоди, наприклад, такої як:**

- порушення цілісності даних;
- втрата важливої інформації;
- попадання важливих даних стороннім особам і т.д.

Кожен збій роботи бази даних може паралізувати роботу цілих корпорацій, фірм, що призведе до великих матеріальних втрат.

Методи захисту баз даних в СУБД умовно можна поділити на дві групи: **основні та додаткові.**

**До додаткових засобів захисту БД можна віднести:**

- вбудовані засоби контролю даних;
- забезпечення цілісності зв’язків таблиць;
- організація спільного використання об’єктів БД в мережі.

**До основних методів захисту відносять:**

- захист паролем;
- шифрування;
- розділення прав доступу до об’єктів БД;
- захист полів і записів таблиць БД.

**Захист паролем** – є самим простим способом захисту БД від несанкціонованого доступу.

Паролі можуть бути встановленні користувачами або адміністраторами. Їх облік і зберігання виконується СУБД. Паролі зберігаються в спеціальних файлах СУБД в зашифрованому вигляді. Після введення пароля користувачу надається доступ до необхідної інформації.

Не дивлячись на простоту парольного захисту, він має ряд недоліків. По-перше, пароль є вразливим, особливо якщо він не шифрується при зберіганні в СУБД. По-друге, користувачу потрібно запам’ятати або записати пароль, а при недбалому відношенні до запису пароль може стати надбанням інших.

Більш сильнішим методом захисту є шифрування. **Шифрування** – це процес обробки інформації за певним алгоритмом в вигляд непридатний для читання, в цілях захисту від несанкціонованого перегляду або використання. Важливою особливістю будь-якого алгоритму шифрування є використання ключа, який стверджує вибір якогось конкретного методу кодування із всіх можливих. Розрізняють два основні методи шифрування: симетричне й асиметричне. В симетричному шифрування один і той же ключ використовується і для шифрування, і для дешифрування. В асиметричних методах застосовуються два ключі. Один з них, несекретний, використовується для шифрування і може публікуватися разом з адресою користувача, другий, секретний, застосовується для дешифрування і відомий тільки одержувачу.

Шифрування забезпечує всі три аспекти безпеки даних: конфіденційність, цілісність і доступність.

В цілях контролю використання основних ресурсів СУБД в багатьох системах є **засоби розділення прав доступу до об'єктів БД**. Права доступу визначають можливі дії над об'єктами. Власник об'єкта, а також адміністратор БД мають всі права. Решта користувачів мають ті права і рівні доступу до об'єктів, якими їх наділили.

**Дозвіл на доступ до конкретних об'єктів бази даних** зберігається в файлі робочої групи. Файл робочої групи містить дані про користувачів групи і зчитується під час запуску. Файл зберігає наступну інформацію:

- імена облікових записів користувачів;
- паролі користувачів;
- імена груп, в які входять користувачі.

Всі вище описані методи є основними, але їх не використання не гарантує повного зберігання даних. Для підвищення рівня безпеки інформації в БД рекомендується використання комплексних заходів.

**Моделі безпеки БД**

Управління доступом в БД включає такі питання, як доступ до таблиць і її полів. Для організації цього доступу використовуються моделі безпеки, які включають дискреційну, мандатну і рольову моделі.

Способом формалізованого представлення дискреційного доступу є матриця доступу або списки управління доступом, що встановлюють перелік користувачів і перелік дозволених операцій відносно кожного об'єкта БД. Можливі декілька підходів до побудови дискреційного управління доступом: децентралізована, централізована та змішана моделі безпеки. Саме змішаний варіант реалізований у більшості СУБД.

Мандатна модель поєднує захист і обмеження прав, що використовуються відносно комп'ютерних процесів, даних і системних пристроїв, та призначена для запобігання їх небажаному використовуванню. Для СУБД мандатна модель безпеки може розширювати або замінювати дискреційний контроль доступу і концепцію користувачів і груп.

Права доступу кожного суб'єкта і характеристики конфіденційності кожного об'єкта відображаються у вигляді сукупності рівня конфіденційності і набору категорій

конфіденційності. Для реалізації безпеки за допомогою мандатної моделі рядкам і стовпцям таблиці БД приписуються мітки, які потім надаються користувачам. Ефективно застосовуватися мандатна модель може тільки разом з дискреційною.

**Рольова модель** – розвиток політики виборного управління доступом, при цьому права доступу суб'єктів системи на об'єкти групуються з урахуванням специфіки їх використання, утворюючи ролі. Управління правами доступу здійснюється як на основі матриці доступу, так і на основі правил, що регламентують поведінку (ролі) користувача та їх активацію під час сеансів.

Рольове розмежування доступу дозволяє реалізувати гнучкі, динамічні правила розмежування доступу. Безпека в цій моделі забезпечується чіткими визначеннями ролей адміністратора БД і користувача БД на права доступу до об'єктів БД і прав на читання, модифікацію, запис і видалення об'єктів. Технологія управління доступом на основі ролей є достатньо гнучкою і потужною, щоб змоделювати як виборне, так і мандатне управління доступом.

**Процедури ідентифікації, аутентифікації і авторизації в СУБД**

Для будь-якої захищеної бази даних обов'язковими є процедури **ідентифікації, аутентифікації та авторизації.**

Сутність процедури **ідентифікації** полягає в призначенні користувачу БД – імені. Ім'я користувача – це деяка унікальна мітка, що відповідає прийнятим угодам і забезпечує однозначну ідентифікацію об'єкта реального світу в просторі об'єктів, що відображаються.

Сутність процедури **аутентифікації** полягає в підтвердженні автентичності користувача, що представив ідентифікатор. У ряді сучасних СУБД використовується:

- **біометрична аутентифікація** – це процес доведення і перевірки автентичності заявленого користувачем імені через пред'явлення користувачем своїх біометричних характеристик (наприклад, відбитки пальців і долоні, звуки голосу, обличчя, відбиток сітківки ока, особливості роботи на клавіатурі, електронний цифровий підпис);
- **парольна аутентифікація** – це процес доведення і перевірки автентичності заявленого користувачем імені шляхом введення ним пароля або парольної фрази. Парольні фрази забезпечують більшу безпеку, ніж короткі паролі, але вимагають більшого часу для введення. Заходами, що дають змогу підвищити надійність парольного захисту є: накладання технічних обмежень, управління терміном дії паролів, обмеження доступу до файлу паролів, обмеження кількості невдалих спроб входу в систему, використання програмних генераторів паролів;
- **аутентифікація із застосуванням токенів. Токен** – це предмет або пристрій, володіння яким підтверджує автентичність користувача.

Ефективність процедур ідентифікації та аутентифікації істотним чином впливає на ефективність системи безпеки в цілому. В процесі **авторизації** встановлюється набір можливих операцій з даними, які може здійснювати користувач.

**<u>Основні поради щодо захисту баз даних підприємств:</u>**

**1. Контролюйте доступ до бази даних.** Запобігти атакам кіберзлочинців допоможуть обмеження дозволів та привілеїв. Крім базових системних дозволів, слід застосувати:

- Обмеження доступу до конфіденційних даних для певних користувачів і процедур, які можуть робити запити, пов'язані з конфіденційною інформацією.
- Обмеження використання основних процедур тільки певними користувачами.
- Уникнення використання і доступу до баз даних в неробочий час.

Також для запобігання атакам зловмисників спеціалісти рекомендують вимкнути всі служби і процедури, які не використовуються. Крім того, базу даних слід розміщувати на сервері, недоступному безпосередньо через мережу Інтернет, щоб запобігти віддаленому доступу зловмисників до корпоративної інформації.

**2. Визначте критично важливі дані.** Першим кроком має стати аналіз важливості захисту для конкретної інформації. Для полегшення визначення місця та способу збереження конфіденційних даних слід зрозуміти логіку і архітектуру бази даних. Не всі дані є критично важливими або потребують захисту, тому на них немає сенсу витрачати час і ресурси.

Спеціалісти також рекомендують провести інвентаризацію баз даних компанії, обов'язково врахувавши всі відділи. Ефективним способом для запобігання втраті інформації може бути фіксація всіх копій і баз даних компанії. Інвентаризація особливо важлива під час виконання резервного копіювання інформації для врахування всіх критично важливих даних.

**3. Шифруйте інформацію.** Після ідентифікації критично важливих даних потрібно застосувати надійні алгоритми шифрування конфіденційної інформації. У разі використання уразливості або отримання доступу до сервера або системи, зловмисники в першу чергу спробують викрасти бази даних, які, зазвичай, містять багато цінної інформації. Кращий спосіб захистити базу даних — зашифрувати її для осіб, які намагаються отримати доступ без авторизації.

**4. Зробіть анонімними непродуктивні бази даних.** Багато компаній інвестують час та ресурси у захист своїх продуктивних баз даних, але при розробці проекту або створення тестового середовища вони просто роблять копію вихідної бази даних і починають використовувати її в середовищах з менш жорстким контролем, тим самим розкриваючи всю конфіденційну інформацію.

За допомогою маскування та анонімізації можна створити аналогічну версію з тією ж структурою, що і оригінал, але із зміненими конфіденційними даними для їх захисту. За допомогою цієї технології значення змінюються за умови збереження формату. Дані можуть бути змінені шляхом змішування, шифрування, переставляння символів або заміни слів. Конкретний метод, правила і формати, залежать від вибору адміністратора, але незалежно від вибору, метод повинен забезпечити неможливість отримати вихідні дані за допомогою зворотньої інженерії.

**5. Проводьте моніторинг активності бази даних.** Аудит і відстеження дій всередині бази даних передбачає знання про те, яка інформація була оброблена, коли, як

і ким. Володіння повною історією транзакцій дозволяє зрозуміти шаблони доступу до даних і модифікацій і, таким чином, допомагає уникати витоку інформації, контролювати небезпечні зміни і виявляти підозрілу активність в режимі реального часу.