Секція 7. Комп'ютерні технології інформаційної безпеки

УДК 681.3.07

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА ЦІЛІСНОСТІ БАЗ ДАНИХ

Брушніцька А.С., Тимошенко Л.М.
Тернопільський національний економічний університет

Захист БД має на меті мінімізувати втрати, викликані заздалегідь передбаченими подіями. Прийняті рішення повинні забезпечувати ефективне використання понесених витрат та усувати зайве обмеження наданих користувачам можливостей.

Комп'ютерні злочини можуть загрожувати будь-якій частині системи, тому наявність необхідних заходів безпеки є життєво важливим.

Системи захисту інформації у інформаційних системах (ІС) призначені для забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів. Для запобігання можливості реалізації загроз ресурсам ІС, в тому числі й СУБД, необхідна розробка і використання в ІС комплексної системи технічного захисту інформації (ТЗІ).

Вимоги до такої системи передбачають централізоване управління засобами і механізмами захисту на основі визначеної власником ІС політики інформаційної безпеки і плану ТЗІ, що її реалізує. Ця задача розв'язується як технічними, так і програмними засобами, а також з використанням спеціально розроблюваних програмних і апаратних засобів ТЗІ.

Для створення структури комплексної системи безпеки БД в ІС потрібно виконати такі етапи:

- визначення технічних каналів витоку інформації;
- побудова моделі загроз і моделі порушника;
- вибір чи розробка методів і засобів захисту інформації;
- оптимізація комплексної системи функціональної безпеки БД в ІС;
- оцінка економічної ефективності комплексної системи функціональної безпеки БД в ІС;
- експлуатація і підтримка в актуальному стані комплексної системи безпеки БД в ІС протягом її життєвого циклу.

Кожна організація повинна установити типи можливих загроз, яким може піддатися її ІС, після чого розробити відповідні плани і необхідні контрзаходи, з оцінкою рівня витрат, достатніх для їхньої реалізації.

Ділові процеси організації, в якій побудовані ІТ для розроблення і впровадження баз і сховищ даних, баз знань і систем комп'ютерної підтримки рішень, можуть бути піддані таким небезпекам, які неодмінно варто враховувати, однак частина з них може мати місце у винятково рідкісних випадках. Проте навіть настільки малоймовірні обставини повинні бути взяті до уваги, особливо якщо їх вплив може виявитися дуже істотним.

Отже, беручи до уваги те, що сервер БД функціонує в ІС, кожний з елементів якої становить потенційну загрозу для конфіденційності та цілісності даних, була розроблена структура локальної мережі, яка б дозволила мінімізувати інформаційні ризики.

Нова структура базується на наступних принципах:

- розміщення СУБД та web-сервера на різних ЕОМ,
- розміщення серверу БД за межами демілітаризованої зони (ДМЗ),
- здійснення шифрування даних між web-сервером і сервером баз даних,
- використання комутаторів замість концентраторів,
- використання САЗ та систем виявлення атак.

Схематично захищений сегмент мережі із СУБД у своєму складі подано на рис. 1.

Відомо, що використання комутаторів замість концентраторів знижує ймовірність перехоплення даних, що передаються по мережі. Коли два хости здійснюють зв'язок через комутатор, між ними утворюється віртуальний канал, трафік в якому не доступний для інших хостів.

Розміщення одного або кількох серверів БД окремо від web-сервера дозволить запобігти розкриттю конфіденційних даних, якщо web-сервер з якихось причин виявиться скомпрометованим.

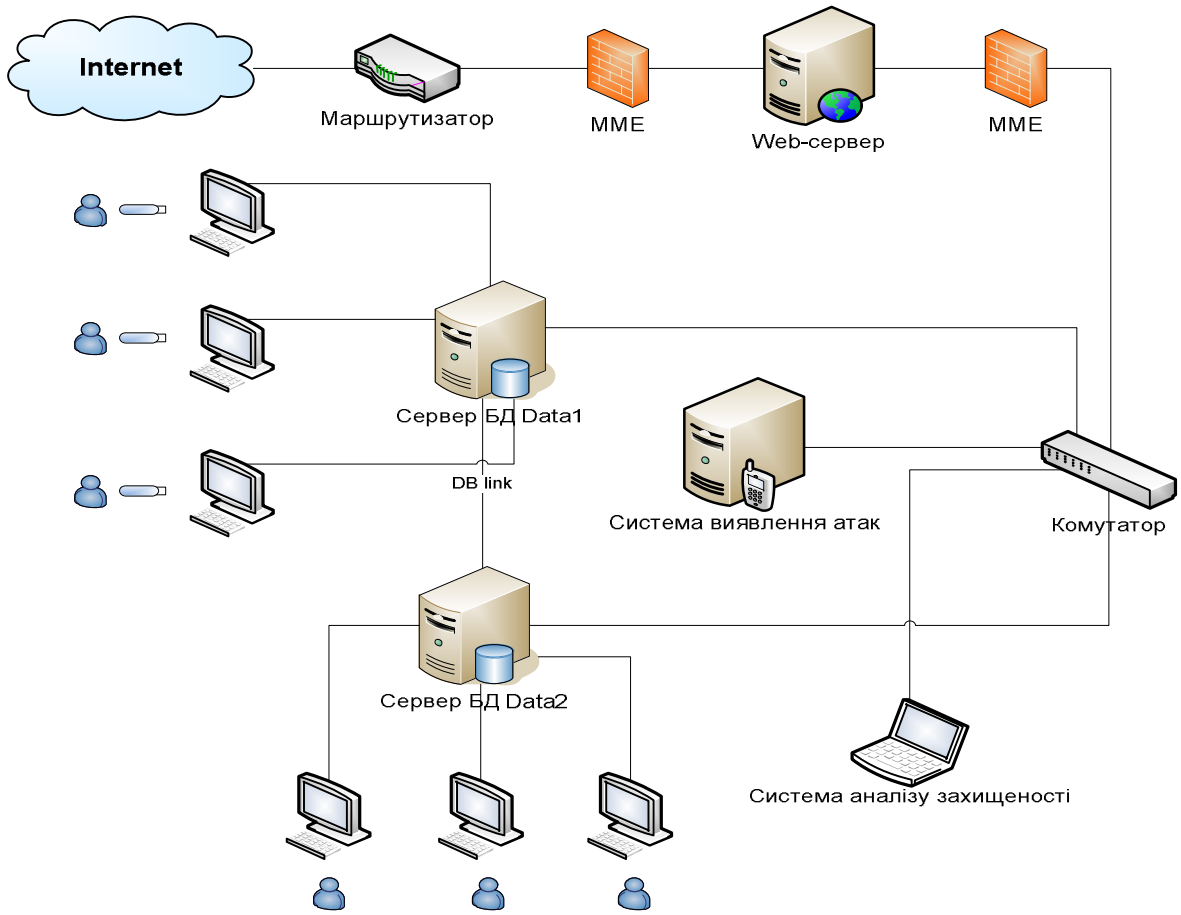

Рисунок 1 - Захищений сегмент локальної мережі

Перепускна здатність мережі навряд чи може стати на заваді розділенню серверів: більшість сегментів мережі працює на швидкостях 100 Мбіт/с або 1 Гбіт/с. На ділянці «клієнтський браузер – web-сервер» зазвичай швидкість нижча, ніж на ділянці «web-сервер – сервер БД».

Одним з найважливіших засобів захисту внутрішніх мережних ресурсів ІС є ММЕ або брандмауери – локальні або функціонально-розподілені програмні чи програмно-апаратні комплекси, які реалізують контроль за інформацією, що надходить в ІС або виходить з неї. Проте слід зауважити, що ММЕ безсилі перед авторизованими користувачами, а також перед встановленими в локальній мережі модемами для віддаленого доступу.

Список використаних джерел

1. Карпінський М., Фурманюк А., Тимошенко Л. Аналіз розповсюджених помилок забезпечення безпеки баз даних//Міжнародний науково-технічний журнал "Вимі-рювальна та обчислювальна техніка в технологічних процесах" №2,2003. - с.128-131.
2. Костров Д. Разграничение информации в современном коммерческом предприятии // Защита информации. Конфидент №2, с. 29-31, 2004.
3. Лопарев С., Шелупанов А. Анализ инструментальных средств оценки рисков утечки информации в компьютерной сети предприятия. // Вопросы защиты информации № 4, 2003.
4. Лукацкий А. Выявление уязвимостей компьютерных сетей. http://www.citforum.ru/internet/securities/vulnerability.shtml
5. Стишенко И. К., Богатырев А. И. К вопросу об информационной безопасности // Науково-технічний журнал «Захист інформації», №2, 2002. - с. 4-9.
6. Тарасов Д. Забезпечення цілісності даних у реляційних структурах. // Інформаційні системи та мережі. Вісник ДУ “Львівська політехніка” №383. - Львів 2009.- с. 213-226.