УДК 004.056

Константинова Л.В.
Кіровоградський національний технічний університет

Аналіз загроз базам даних та огляд методів їх запобігання

Зараз, в часи стрімкого розвитку кіберпростору, зростає необхідність застосування інформаційних технологій. Застосування баз даних (БД) для підприємств та організацій є оптимальним методом для роботи з великими обсягами інформації. Згідно даним з статистики в останні роки кількість витоків даних неухильно зростає [1]. Проаналізувавши частоту випадків злому баз даних можна стверджувати, що захист даних від несанкціонованого доступу є одною з пріоритетних задач при проектуванні будь-якої інформаційної системи. Для вирішення цих задач необхідно провести аналіз загроз баз даних та методів і засобів для їх запобігання.

Руйнування комп'ютерних сховищ корпоративних даних або втрата, просто тимчасова недоступність цих даних може стати причиною справжньої катастрофи для організації чи підприємства [2].

Наприклад, в 2016 році в Дніпрі ріелтори фіксують випадки зломів баз даних реєстру нерухомості, наслідком чого законні власники квартир позбавляються своєї власності [3].

В 2016 році американська компанія ThreatConnect, яка займається питаннями кібербезпеки, розслідувала зломи електронної бази виборців, які відбулися в двох американських штатах і прийшла до висновку, що атаку провели з тієї ж IP адреси, з якої атакували Україну, Туреччину і Німеччину [4].

У 2013 році міністр закордонних справ Фінляндії заявив про випадки злому своєї бази даних [5].

У 2016 р.WADA звинувачує Росію у зломі секретних баз даних про застосування допінгу спортсменами США. За словами чиновників WADA, яких хакери з міжнародної групи Fancy Bear викрили в санкціонуванні прийому допінгу американськими спортсменами, заявляють, що система антидопінгового адміністрування та менеджменту (ADAMS) дійсно була зламана, і дійсно в ній знаходилися «довідки-дозволу» на використання окремими американськими спортсменами справжніх коктейлів із заборонених медпрепаратів [6].

У 2014 році газета New York Times з посиланням на високопоставлених американських чиновників повідомила, що китайські хакери в березні провели велику атаку на сховища Управління кадрової служби США і заволоділи інформацією про федеральних службовців, які зверталися в державні структури за наданням секретної інформації. Як тільки відповідні служби виявили злом, доступ до файлів був закритий. Залишається невідомим, яку інформацію і в якій кількості змогли роздобути хакери [7].

Чисельність повідомлень про випадки злому баз даних велика, але більша кількість компаній не оголошує такі випадки для збереження іміджу.

База даних являє собою найважливіший корпоративний ресурс, який повинен бути належним чином захищений за допомогою відповідних засобів і методів. Щоб оперативно вживати заходів, що знижують ступінь ризику, тобто потенційну можливість втрати або

пошкодження даних необхідно вивчити відповідні загрози.

Відомі наступні потенційні загрози баз даних (БД) [8]:

- Викрадення і фальсифікація даних;
- Втрата конфіденційності (порушення таємниці);
- Порушення недоторканності особистих даних;
- Втрата цілісності;
- Втрата доступності.

Через зв'язки загроз між собою, як правило, порушення захищеності системи в одному напрямку часто викликають зниження захищеності системи у інших напрямках.

Викрадення і фальсифікація даних можуть відбуватися не тільки в середовищі бази даних - вся інформаційна система тієї чи іншої організації може бути під цією загрозою. Тому, будь-яка інформаційна система потребує постійного спостереження за всіма можливими каналами витоку інформації, якими потенційно володіє [2].

Поняття конфіденційності означає необхідність збереження даних в таємниці. Конфіденційна інформація - це інформація з обмеженим доступом, якою володіють, користуються, розпоряджаються окремі фізичні, юридичні особи або держава, порядок доступу до якої встановлюється ними.

Втрата цілісності даних призводить до їх спотворення або руйнування, що може мати найсерйозніші наслідки для подальшої роботи організації (наприклад, втрата надійних позицій в конкурентній боротьбі).

Втрата доступності даних для організації, що функціонує в безперервному режимі означатиме: або дані, або система, або те й інше одночасно виявляться недоступними користувачам. Це може поставити під небезпеки і фінансове становище організації, і всілякі системи управління, що використовують бази даних для своїх потреб.

Не торкаючись загальних питань інформаційної безпеки, а також загальних методів і засобів захисту інформації, розглянемо традиційні методи і засоби захисту даних, реалізовані за допомогою можливостей, закладених в системах управління базами даних, з урахуванням особливостей реалізації схеми бази даних з універсальною моделлю даних.

Засоби і методи захисту баз даних відрізняються один від одного в залежності від систем керування базами даних (СКБД), але в тій чи іншій мірі досить часто зустрічаються наступні [2]:

-авторизація користувачів;
-застосування представлень;
-резервне копіювання та відновлення;
-підтримка цілісності;
-шифрування;
-застосування відказостійких апаратних засобів.

Для подолання проблем забезпечення інформаційної безпеки СКБД необхідно перейти від методу закриття вразливостей до комплексного підходу забезпечення безпеки сховищ інформації. Основними етапами цього переходу повинні стати наступні положення [9].

1. Розробка комплексних методик забезпечення безпеки сховищ даних на поточному етапі.

Створення комплексних методик дозволить застосовувати їх (або їх відповідні версії) при розробці сховищ даних і користувальницького ПЗ.

2. Оцінка і класифікація загроз і вразливостей СКБД.

Спеціалізована класифікація загроз і вразливостей СКБД дозволить упорядкувати їх для подальшого аналізу і захисту, дасть можливість встановити залежність між вразливостями і причинами (джерелами) їх виникнення. В результаті при введенні конкретного механізму в СКБД з'явиться можливість встановити і спрогнозувати пов'язані з ним загрози і заздалегідь підготувати відповідні засоби забезпечення безпеки.

3. Розробка стандартних (застосовуються до різних СКБД без внесення змін або з мінімальними змінами) механізмів забезпечення безпеки.

Стандартизація підходів і мов роботи з даними дозволить створити мультиплатформені засоби забезпечення безпеки, які застосовуються до різних СКБД. З одного боку, це методичні та теоретичні підходи, що застосовуються в рамках моделі даних. На сьогоднішній день є напрацювання таких механізмів для реляційної моделі, однак вони не вирішують всіх нагальних питань безпеки. З іншого - це розробка теоретичного базису для нових СКБД, зокрема, конкретизація і формалізація агрегатних моделей даних. Поява готових програмних засобів багато в чому залежить від виробників і розробників СКБД і їх слідування стандартам, а також достатності визначених у стандарті засобів для побудови розвинених механізмів безпеки.

4. Розробка теоретичної бази інформаційного захисту систем зберігання і маніпулювання даними.

В Україні найбільше від кібератак страждають бази даних впливових медіа, фінансових інститутів та державних установ. При цьому на сьогодні зростає не тільки кількість атак на інформаційну інфраструктуру, але і їх складність. Щоб оперативно вживати заходів, що знижують ступінь ризику, тобто потенційну можливість втрати або пошкодження даних необхідно вивчати відповідні загрози, аналізувати відповідність методів протидії та до кіберзахисту сховищ даних підходити комплексно.

Список використаних джерел

1. *Исследование утечек информации за первое полугодие 2015 года URL:* https://www.infowatch.ru/analytics/reports/16340
2. *Традиционные методы и средства защиты данных, реализованные в базе данных с универсальной моделью данных [Текст] / Л. С. Сорока, В. И. Есин, М. В. Есина // Академія митної служби України. Вісник Академії митної служби України. Серія "Технічні науки". 2010 р. № 2 (44) / Академія митної служби України. - Д., 2010. - С. 7*
3. *Информационное агентство Мост Днепр 05.09.2016 URL:* http://most-dnepr.info/press-centre/announcements/139515.htm.
4. *Сводка независимых новостей 3.09.2016 URL: http://svodka.net/ekonomika/obschestvo-ekonomika/17504*
5. *Подробности 1.11.2013 URL:* http://podrobnosti.ua/939856-mid-finljandii-zajavil-o-sluchajah-vzloma-svoej-bazy-dannyh.html
6. *Военное обозрение 14.09.2016 URL:* https://topwar.ru/100681-wada-obvinyaet-rossiyu-vo-vzlome-sekretnyh-baz-dannyh-o-primenenii-dopinga-amerikanskimi-sportsmenami.html
7. *РИА Новости 14.08.2014 URL:* https://ria.ru/spravka/20140814/1019983404.html
8. *Есин В. И. Безопасность информационных систем и технологий / Есин В. И., Кузнецов А. А., Сорока Л. С. – Х. : ЭДЭНА, 2010. – 656 с.*
9. *Полтавцева М. А., Хабаров А. Р. Безопасность баз данных: проблемы и перспективы Международный журнал Программные продукты и системы №3 2016. URL: http://www.swsys.ru/index.php?page=article&id=4175.*