https://cyberleninka.ru/article/v/sotsialnaya-inzheneriya-kak-professiya (дата звернення: 30.10.2018).

2. Ногалес К. Социальная инженерия // 4brain. 12 Дек 2017. URL: https://4brain.ru/blog/социальная-инженерия/ (дата звернення: 30.10.2018).

3. Bezmaly V. Как защищать сотрудников от угроз социальной инженерии // IT-community: IT сообщество Украины. 23.07.2014. URL: https://it-community.in.ua/2014/07/kak-zashhishhat-sotrudnikov-ot-ugroz-sotsialnoj-inzhenerii.html/ (дата звернення: 30.10.2018).

4. Bezmaly V. Технологи социальной инженерии // IT-community: IT сообщество Украины. 29.10.2014. URL: https://www.it-community.in.ua/2014/10/tehnologi-sotsialnoj-inzhenerii.html/ (дата звернення: 30.10.2018).

5. Нам'ясенко В. М. Соціальна інженерія як одна із загроз економічній безпеці, що спричиняє негативний вплив на ефективність діяльності підприємства. *Економіка та держава*. 2016. № 3. С. 90-92. URL: http://www.economy.in.ua/pdf/3_2016/21.pdf (дата звернення: 30.10.2018).

6. Соціальна інженерія (безпека) // Вікіпедія: вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Соціальна_інженерія_(безпека) (дата звернення: 30.10.2018).

Одержано 31.10.2018

УДК 681.3.06

Артур Геннадійович ПЛАКСЮК,
курсант 2 курсу групи Ф4-202 факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ

ПРОБЛЕМАТИКА ЗАХИСТУ ІНФОРМАЦІЇ В БАЗІ ДАНИХ

Можна з достовірністю стверджувати, що більшість прикладних програм, які призначені для виконання будь-якої корисної роботи, тим або іншим чином використовують структуровану інформацію або, іншими словами, упорядковані дані. Такими даними можуть бути, наприклад, списки замовлень на той чи інший товар, списки пред'явлених і оплачених рахунків, список телефонних номерів ваших друзів, або розклад руху автобусів у вашому місті .

При комп'ютерній обробці інформації, упорядковані будь-яким способом, дані зберігаються в базах даних (БД) – особливих файлах, використання яких разом із спеціальними програмними засобами дозволяє користувачеві переглядати необхідну інформацію, так само, як і при необхідності, маніпулювати нею, наприклад, додати, змінити, копіювати, видалити, сортувати і т.д. Просто кажучи, дати визначення бази даних можна наступним чином: база даних – це набір інформації, організованої будь-яким способом.

В сучасному світі жодна організація, підприємство і т.д. не обходиться без використання БД які містять найрізноманітнішу інформацію. Таким чином в БД може зберігатися дуже делікатна або

конфіденційна інформація, яка потребує серйозного підходу до її захисту.

Захист БД – це забезпечення захищеності БД від будь-яких передбачуваних чи непередбачуваних загроз з використанням різних комп'ютерних та некомп'ютерних засобів.

Поняття захисту застосовується не тільки до збереженої в БД інформації. Діри в системі захисту можуть виникнути і в інших частинах системи, що, у свою чергу, піддає небезпеці і власне БД. Відповідно, захист БД повинен охоплювати використовуване устаткування, програмне забезпечення, персонал та власне дані.

Для ефективної реалізації захисту необхідні відповідні засоби контролю, які визначаються конкретними вимогами, що випливають з особливостей експлуатується системи.

Розглянемо проблеми захисту БД з точки зору таких потенційних небезпек: викрадення та фальсифікація даних; втрата конфіденційності (порушення таємниці); порушення недоторканості особистих даних; втрата цілісності; втрата доступності.

Указані ситуації відзначають основні напрями, в яких керівництво має вживати заходів, що зменшують ступінь ризику, тобто потенційна можливість втрати або пошкодження даних.

Викрадення та фальсифікація даних можуть відбуватися не тільки в середовищі БД – вся організація, так чи інакше, піддається цій небезпеці. Однак дії по викраденню або фальсифікації інформації завжди здійснюються людьми, тому основну увагу треба звернути на скорочення загального числа зручних ситуацій для виконання подібних дій. Викрадення і фальсифікація необов'язково пов'язані з зміною будь-яких даних, що справедливо і щодо втрати конфіденційності або порушень незаконності особистих даних.

Втрата конфіденційності і порушення неправомірності особистих даних. Поняття конфіденційності означає необхідність збереження даних в таємниці. Як правило, конфіденційні вважаються даними, які є критичними для всієї організації, тоді як поняття недоторканості даних стосується вимог захисту інформації про окремих працівників. Як наслідок, порушення в системі захисту, що викликало втрату конфіденційності даних, може бути причиною втрати позицій у конкурентній боротьбі, тоді як слідство порушення особистих даних працівників буде юридичним заходом, прийнятим щодо організації.

Втрата цілісності та втрата доступності даних. Втрата цілісності даних призводить до викривлення або руйнування даних, що може мати критичний вплив на подальшу роботу організації. В даний час безліч організацій функціонує в безперервному режимі, надаючи свої послуги клієнтам по 24 години на добу і по 7 днів на тиждень. Втрата доступності даних – це коли будь-які дані, або система, або те й інше, одночасно опиняються недоступними для користувачів, що може піддати небезпеці подальше існування організації. У деяких випадках

ті події, які служили причиною переходу системи в недоступний стан, можуть одночасно викликати і руйнування даних у базі.

Таким чином, загроза може бути викликана ситуацією або подією, здатною принести шкоду організації, причиною якої може послужити людина, подія чи збіг обставин. Навмисні загрози завжди здійснюються людьми і можуть бути вчинені як авторизованими, так і неавторизованих користувачів, причому останні можуть не належати організації. Будь-яка небезпека повинна розглядатися як потенційна можливість порушення системи захисту, яка в разі своєї реалізації може призвести до того чи іншого негативного результату.

Виділяють такі основні методи захисту БД: захист паролем; шифрування даних і програм; розмежування прав доступу до об'єктів БД; захист полів і записів таблиць БД.

Захист паролем представляє собою простий і ефективний спосіб захисту БД (баз даних) від несанкціонованого доступу. Паролі встановлюються користувачами чи адміністраторами БД. Облік і зберігання паролів виконується самою системою управління базами даних (СУБД). Зазвичай паролі зберігаються в окремих системних файлах СУБД в зашифрованому вигляді. Після вводу пароля користувачу СУБД надаються всі можливості по роботі з БД.

Паролі з їх головною перевагою – простотою і звичністю при правильному використанні можуть забезпечити прийнятний для багатьох компаній рівень безпеки. Надійність пральний захисту ґрунтується на наступних вимогах: пароль повинен являти собою комбінацію букв, цифр або спеціальних знаків; довжина пароля повинна бути не менше шести символів; паролі повинні часто змінюватися і зберігатися в таємниці.

Шифрування – перетворення тексту, який можна прочитати в незчитуваний за допомогою деякого алгоритму; застосовується для захисту вразливих даних. Процес дешифрування відновлює дані в початковий стан. Права доступу визначають можливість дії над об'єктом. Власник об'єкта – користувач, який створив об'єкт. Решта користувачів до різних об'єктів можуть мати різні рівні доступу. Дозвіл на доступ до конкретних об'єктів БД зберігається в файлі робочої групи. Файл робочої групи містить дані про користувачів групи: імена облікових записів користувачів, паролі користувачів, імена груп, в які входять користувачі.

Права доступу до таблиць включають: перегляд (зчитування) даних; зміна (редагування) даних; додавання нових записів; додавання і видалення записів; зміна структури таблиці.

Права доступу до полів таблиці визначають: повну заборону доступу; тільки читання даних; дозвіл всіх операцій (перегляд, введення значень, видалення і зміна).

Права доступу до форм забезпечують: виклик для роботи і проектування режиму Конструктора та захист окремих елементів.

Додаткові засоби захисту реалізують: вбудовані засоби контролю значень даних відповідно до типу; підвищення достовірності даних, що вводяться; забезпечення цілісності зв'язків таблиці; організацію спільного використання об'єктів БД в мережі.

Наступним способом обслуговування бази даних є резервне копіювання. Основним призначенням резервного копіювання БД є запобігання втрати інформації і реалізується шляхом одноразового або періодичного копіювання та архівування найбільш цінної інформації. Резервне копіювання полягає в створенні резервної копії БД і розміщенні на допоміжних носіях інформації: жорстких дисках, дискетах, накопичувачах на оптичних дисках, магнітних стрічках.

При організації резервного копіювання адміністратор вирішує такі питання: які пристрої вибрати для резервного копіювання; коли і з якою частотою створювати резервні копії.

В результаті досліджень сформульовані загальні вимоги до безпеки БД, перспективні шляхи дослідження і розвитку систем захисту БД. При цьому, захист баз даних повинно здійснюватися поетапно, починаючи з прийняття базових заходів. Описані вище методи здатні певною мірою забезпечити конфіденційність і цілісність даних, однак їх використання не гарантує повної безпеки даних. Для підвищення рівня безпеки інформації в базі даних рекомендується використання комплексних заходів, включаючи інтеграцію СУБД зі спеціальними програмними продуктами для захисту інформації.

Список бібліографічних посилань

1. Полтавцева М. А., Хабаров А. Р. (Безопасность баз данных: проблемы и перспективы. Международный научно-практический журнал «*Программные продукты и системы*». 2016. № 3. С. 36-41. URL: http://www.swsys.ru/index.php?page=article&id=4175&lang= (дата звернення: 30.10.2018).

2. Проблемы защиты базы данных // Студопедия. URL: https://studopedia.su/9_84613_problemi-zashchiti-bazi-dannih.html (дата звернення: 30.10.2018).

3. Увайсова З. М., Билалова И. М. Защита и безопасность баз данных // VII Международная студенческая научная конференция «Студенческий научный форум – 2015». URL: https://scienceforum.ru/2015/article/2015015774 (дата звернення: 30.10.2018).

4. Разработка БД в среде Visual Basic. Урок 1. Введение в базы данных // CODENET: Все для программиста! URL: http://www.codenet.ru/progr/vbasic/vb_db/1.php (дата звернення: 30.10.2018).

5. С чего начинается защита базы данных? // DataArmor. URL: https://www.dataarmor.ru/c-чего-начинается-защита-базы-данных/ (дата звернення: 30.10.2018).

6. Методы защиты бд: защита паролем, шифрование, разграничение прав доступа // StudFiles: Файловый архив студентов. URL: https://studfiles.net/preview/5405333/page:36/ (дата звернення: 30.10.2018).

Одержано 01.11.2018