Проведення моніторингу активності БД. 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.

Перегляд існуючої системи на предмет будь-яких відомих або невідомих уразливостей та визначення та реалізація дорожньої карти/плану їх зменшення.

Можна зробити висновок що використання лише якогось певного методу не може гарантувати повного зберігання даних. Тому для підвищення рівня безпеки інформації в БД рекомендовано використання комплексних заходів.

Розробки в сфері безпеки БД є дуже актуальними та потребують майже не щоденного вдосконалення.

Особливої актуальності ця проблема набула в час російсько-української війни, коли задля безпеки на рівні держави вжили максимальних заходів - закрили повний доступ для всіх державних реєстрів, тим самим відсікли їх від глобальної мережі.

Список використаних джерел:

1. Касянчук, Н. В., Ткачук Л. М. Захист інформації в базах даних. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/download/7001/5715. 2019
2. Як створити надійний пароль — рекомендації спеціалістів ESET. URL: https://eset.ua/ua/news/view/649/nadezhnyy-parol-sposoby-sozdaniya-parolya- ot-spetsialistov-eset
3. Шифрування та захист баз даних. URL: https://iitd.com.ua/shifruvannj a-ta-zahist-baz-danih/
4. Системи управління базами даних. URL: http: //rodak.if. ua/komptech/lection4 .htm
5. Защита баз данных – залог безопасности корпоративной сети. URL: https: //eset.ua/ua/blog/view/14/

Науковий керівник: доцент Задерейко О.В.

ЗАСОБИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ

Максимчук А.Ю.

студентка 1 курсу судово-адміністративного факультету факультету Національного університету «Одеська юридична академія»

Сьогодні інтернет всюди проник у наше життя і діяльність. Користувачі використовують його кожен день, починаючи з соціальних мереж і до онлайн-банкінгу. Також цей ресурс який використовується для навчання і праці.

Сучасні користувачі мають доступ до інтернету майже з усіх власних електронних приладів: комп'ютери, смартфони, планшети, телевізори тощо.

Саме цей факт обумовлює необхідність знань про безпеку в мережі Інтернет [1].

Кожен користувач має віднайти для себе оптимальні засоби захисту своїх персональних даних, щоб в подальшому житті їх не могли використовувати зловмисники.

До персональних даних може бути віднесені не тільки ім'я прізвище чи дата народження. У законодавстві України так називають будь-яку інформацію яка допомагає ідентифікувати особистість користувача. Тобто персональними даними можуть бути:

- ім'я та прізвище;
- дата та місце народження;
- сімейний стан;
- паспортні дані;
- професія тощо.

Також варто зазначити, що паролі та акаунти не являються персональними даними, бо вони не несуть конкретну інформацію про особу. Але можуть бути використаний злочинцями для здобуття важливої інформації.

Захист особистих даних

Пересічному користувачеві мережі Інтернет рекомендовано наступні кілька способів збереження персональної інформації [2]:

1. Створення складних паролів. Він має містить в собі букви цифри, великі й малі, не менше ніж 12 символів. А також важливо, що пароль не містив особливих даних таких як: прізвище або дата народження.

2. Оновлення програмного забезпечення. Необхідно своєчасно оновлювати програмне забезпечення навпаки, Адже розробники ретельно слідкують за наявністю можливих загроз і намагаються захистити свій продукт.

3. Використання двофакторної аутентифікації. Найбільш дієвий критерій в для захисту даних. Різні мережеві сервіси мають можливість підтвердження двофакторної автентифікації. Частіше це робиться за допомогою СМС повідомлення. Але існує можливість його перехоплення. Замість СМС краще спробувати такі застосунки як Google Authenticator.

4. Правила користування публічним Wi-Fi. В суспільних місцях, необхідно користуватися VPN-з’єднанням.

5. Спостереження за адресним рядком. Необхідно слідкувати за наявністю безпечного з’єднання підчас web-серфінгу. Безпечніше, щоб web-браузер використовував HTTPS з’єднання.

6. Конфіденційність у соцмережах. При користуванні соціальними мережами необхідно пам'ятати, що будь-яка інформація, яку користувач вирішив оприлюднити у себе на сторінці, автоматично стає загальнодоступною.

Справа в тому, що кожна соцмережа є безцінним джерелом інформації для зловмисників, які збирають персональні дані, які вони потім використовують для обману і шахрайства. Тому дуже важливо правильно налаштувати конфіденційність профілю користувача будь-яких соцмережах.

7. Захищеність електронної Пошти. Як правило в електронній поштовій скриньці зберігаються "ключі" від більшості облікових записів користувача, так як процедура відновлення пароля найчастіше здійснюється саме за допомогою email-повідомлень. Тому життєво необхідно захистити свою основну поштову скриньку, до якої прив'язані інтернет-банк і найважливіші мережеві сервіси. Якщо користувач бажає зареєструватися на сайті знайомств або в якомусь сумнівному сервісі, краще створити запасну поштову скриньку.

В статті 24 Закону України "Про захист персональних даних" вказано що "Власники, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкової втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних" [3]. Тобто, по-перше, користувачі самі несуть відповідальність за збереження їх персональних даних.

Отже, якщо користувач будете дотримуватись вказаних вимог тоді його персональні дані будуть більш захищеними.

Список використаних джерел:

1. Безпека в Інтернеті, що потрібно знати. URL: https://pon.org.ua/novyny/5427-bezpeka-v-nternet-scho-potrbno-znati.html
2. 5 шляхів захисту особистих даних в Інтернеті. URL: https://beetroot.academy/blog/general/5-shlyahiv-zahistu-osobistih-danih-v-interneti
3. Законодавство України. Закон України "Про захист персональних даних". URL: https://zakon.rada.gov.ua/laws/show/en/2297-17#Text

Науковий керівник: доцент Задерейко О.В.

АНАЛІЗ АКТИВНОСТІ КОРИСТУВАЧА ЗА ПРОФІЛЕМ БРАУЗЕРА CHROME

Малюта В. В.

студент 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Років 20 тому, коли Інтернет з долі обраних почав стрімко перетворюватися в масове явище, перед тисячами новоспечених користувачів виникло питання: яку пошукову систему використовувати?