Секція 1

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ

Резніков А.О.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Землянко Г.А.

Актуальність. З ростом популярності соціальних мереж зростає і питання захисту персональних даних. Коли користувачі реєструються в соціальних мережах, вони, як правило, надають особисту інформацію, таку як ім'я, адреса та дата народження. Ця інформація потім зберігається на серверах соціальної мережі.

Відомо, що хакери націлені на соціальні мережі, щоб отримати доступ до цієї особистої інформації. Отримавши доступ до облікового запису користувача, вони можуть переглядати його особисті дані, такі як список контактів і приватні повідомлення[1]. Виходячи з цієї інформації, було виділено необхідність розглянути та застосувати методи захисту особистої інформації у розробці соціальної мережі.

Мета роботи: полягає у дослідженні методів захисту персональних даних в соціальних мережах.

Основні положення. Існує багато методів захисту особистих даних у веб-додатках. Деякі поширені методи включають в себе: використання SSL/TLS для шифрування даних під час передачі, зберігання даних у зашифрованому форматі, використання механізмів контролю доступу для обмеження доступу до даних.

Для захисту під час передачі даних між браузером користувача та сервером в соціальній мережі використовується протокол HTTPS, який являє собою звичайний HTTP, що працює через шифровані транспортні механізми SSL/TLS[2]. Це важливо, оскільки дані часто передаються через мережі, які не є повністю захищеними. Коли дані зашифровані, навіть якщо хакери зможуть перехопити дані, наприклад при використанні користувачем скомпрометованої мережі, вони не зможуть розшифрувати та переглянути їх без відповідних ключів.

Не менш важливим є захист даних, що зберігаються на сервері. Для цього використовуються кілька методів. База даних і веб-сервер знаходяться на різних серверах, при чому тільки веб-сервер має доступ до мережі інтернет, база даних пов'язана з ним тільки по приватній мережі. Це дозволяє обмежити несанкціонований доступ до бази даних і захистити дані при передачі між БД і сервером. Дані у базі даних зберігаються у зашифрованому форматі. Коли дані потрібні, вони розшифровуються за допомогою відповідних ключів. Це гарантує, що навіть якщо хакери зможуть отримати доступ до бази даних, вони все одно не зможуть переглянути дані.

Іншим поширеним методом є використання механізмів контролю доступу для обмеження доступу до даних. Наприклад, доступ до конфіденційних даних користувачів є тільки у адміністраторів, у чиї обов'язки входить робота з даними користувачів.

У самій соціальній мережі користувач може отримати доступ лише до своїх даних та даних якими явно поділилися інші користувачі. Також користувач може запросити надання архіву з усіма даними, що зберігаються про нього, а також запросити видалення свого облікового запису та всіх даних пов'язаних з ним, як зазначено в GDPR[3].

Висновки. Розглянуті в цій роботі способи захисту персональних даних у соціальних мережах - це лише деякі з багатьох способів захисту даних користувачів. Важливо пам'ятати, що за безпеку даних користувачів відповідає як соціальна мережа, так і сам користувач. Користувачі повинні усвідомлювати ризики обміну особистими даними в Інтернеті та вживати заходів для захисту власних даних, наприклад, використовувати надійні паролі та не ділитися конфіденційною інформацією з іншими особами. Соціальні мережі ж повинні надавати користувачам можливості контролювати свої дані та забезпечувати наявність адекватних заходів безпеки для захисту даних користувачів.

Список літератури

1. 5 Of the Biggest Hacks in Cybersecurity History. *Discover Magazine*. URL – https://www.discovermagazine.com/technology/5-of-the-biggest-hacks-in-cybersecurity-history (дата звернення: 10.11.2022);
2. HTTPS. *Wikipedia*. URL: https://uk.wikipedia.org/wiki/HTTPS (дата звернення: 15.11.2022);
3. Регламент (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних).

Відомості про авторів

Резніков Андрій Олександрович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 0975418608, a.reznikov@student.csn.khai.edu
Землянко Георгій Андрійович, асистент кафедри комп’ютерних систем, мереж і кібербезпеки. g.zemlynko@csn.khai.edu