Граф М. С., Ph.D, зав. кафедри КН
Райковський В. А., магістрант
Державний університет «Житомирська політехніка»

ОБҐРУНТУВАННЯ ВИБОРУ АЛГОРИТМУ ПОБУДОВИ БЕЗПЕЧНИХ ВЕБ-ДОДАТКІВ ДЛЯ ОБМІНУ ПОВІДОМЛЕННЯМИ

Постановка задачі. Протягом останніх років цифрове листування стало основою сучасного спілкування, охоплюючи як особисті, так і професійні аспекти життя. Саме тому, безпека такого спілкування займає ключову позицію, адже від цього залежить захист особистих даних, конфіденційної інформації та ділових секретів.

Сьогодні бізнес активно прагне інтегрувати можливості обміну повідомленнями в корпоративні інформаційні системи, що використовуються в їхній роботі. Такі інтеграції дозволяють суттєво підвищити ефективність внутрішньої комунікації.

Розробка веб-додатка для обміну повідомленнями з можливістю інтеграції його в корпоративні інформаційні системи дозволить забезпечити ефективну комунікацію всередині компанії, а отже, підвищивши продуктивність роботи. Ключовим аспектом такої розробки є використання алгоритмів та інноваційних методів побудови безпечних веб-додатків для обміну повідомленнями, що гарантує надійний захист корпоративної інформації та конфіденційних даних.

Мета дослідження. Аналіз існуючих алгоритмів та методів розробки безпечних веб-додатків для обміну повідомленнями.

Огляд алгоритмів та методів забезпечення безпеки веб-додатків. При розробці веб-додатків особливо важливо забезпечити конфіденційність та безпеку даних користувачів, зокрема у програмних продуктах, що обробляють особисту інформацію [1]. Веб-додатки для обміну повідомленнями є прикладом таких продуктів.

На рисунку 1 зображена структурна схема, що являє комплекс дій необхідний щоб забезпечити надійність та безпеку веб-застосунків.

У цьому дослідженні акцентуємо увагу на шифруванні даних та його важливості для забезпечення безпеки веб-додатків для обміну повідомленнями. Розглянемо алгоритм End-to-End Encryption та особливості його застосування.

Рисунок 1 – Безпека веб-додатку

End-to-End Encryption (E2EE) — підхід, що передбачає доступ до повідомлень тільки відправнику та отримувачу, шляхом обміну публічними ключами шифрування. Прикладом використання данного алгоритму є Signal Protocol, який використовується в таких популярних месенджерах, як WhatsApp та Signal. Саме цей метод шифрування дозволяє захистити данні користувачів максимально якісно, адже ніхто крім відправника не може розшифрувати повідомлення, тобто будь-хто зі злочинними намірами не зможе отримати доступу до повідомлень.

Розглянемо алгоритм E2EE на прикладі обміну повідомленнями між двома користувачами. На початку кожен користувач генерує пару ключів: публічний (для обміну) і приватний (для розшифрування). Обмін ключами відбувається за допомогою серверу. Далі відбувається створення сесійного ключа, саме він використовується для шифрування повідомлення перед відправкою, користувачі обмінюються створеними ключами на основі алгоритму Диффі-Хелмана, за рахунок цього вони можуть створити спільний ключ не виконуючи при цьому передачу самого ключа через мережу. Відправник шифрує повідомлення використовуючи сесійний ключ та симетричне шифрування. Отримувач розшифровує повідомлення за допомогою сесійного ключа, який розшифрував використавши приватний ключ. Після кожного відправленого повідомлення сесійний ключ оновлюється, тим самим підвищуючи безпеку. Також є можливість підвищити безпеку алгоритму шляхом використання іншого протоколу узгодження двох раундів секретних ключів алгоритму Диффі-Хелмана [2], тому застосування цього підходу є оптимальним варіантом для підвищення надійності.

Використання алгоритмів та інноваційних методів безпеки, таких як End-to-End Encryption допоможе забезпечити безпеку та конфіденційність даних користувачів. Впровадження описаного алгоритму у веб-додаток для обміну повідомленнями дозволить гарантувати, що доступ до повідомлення отримає тільки відправник та отримувач.

Список використаних джерел:

1. Hoffman A. Web Application Security: Exploitation and Countermeasures for Modern Web. Gravenstein Highway North, Sebastopol: O’Reilly Media, Inc, 2024.
2. Pundir M., Kumar A., Choudhary S. Efficient Diffie Hellman Two Round Secret Key Agreement Protocol. 2023 1st International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP). Bhopal, India, 2023. С. 7–10.