УДК 004.05

В. КАПЕЛЮШНИЙ, Н. КУШНІРЕНКО

Національний університет Одеська політехніка

ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СТВОРЕННЯ ТА ПРОВЕДЕННЯ ОПИТУВАНЬ

Вступ: в умовах зростання впливу мережі Інтернет на життя людей, захист особистої та конфіденційної інформації займає вагоме місце. З розвитком та змінами алгоритмів захисту інформації розвиваються і способи обходу та злому захисту інформації. В результаті чого, витік інформації, яка становить таємниці може призвести до непоправних наслідків. На сьогодні багато процесів переведено в онлайн формат, тому постає питання необхідності захисту персональних даних. Одним з таких процесів є проведення опитувань. Хоч і для простих тестів, які містять лише прізвище та ім'я учня, не так важливо забезпечення безпеки, але для опитування, наприклад, працівників державних організацій та інших установ, які можуть нести в собі конфіденційну інформацію, дане питання є доволі актуальним.

Мета: проаналізувати захист найпоширеніших платформ для проведення тестування в режимі онлайн.

1. Аналіз безпеки програмного забезпечення для адміністрування опитування Google Forms

Додаток Google Forms надає можливість створювати та керувати опитуваннями в режимі реального часу, співпрацюючи з іншими користувачами. Після чого, опрацьовувати отримані дані в електронній таблиці. Корпорація Google гарантує забезпечення безпеки та конфіденційності всієї інформації, яку отримує для подальшого опрацювання. Forms працює повністю у хмарному середовищі, тому користувачам не потрібно використовувати локальні файли наражаючи свій пристрій на ризики [1].

Google Forms надають можливість встановлювати різні рівні доступу для опитувань, які дозволяють контролювати права заповнення, перегляду та редагування опитувань, що також важливо для збереження конфіденційності даних.

У Google пропонується двофакторна аутентифікація, яка знижує ризик несанкціонованих доступів до облікових записів, особливо це важливо, якщо облікові записи адміністраторів містять конфіденційну інформацію про інших користувачів.

Google Forms під час обміну даними між користувачем та своїми серверами використовує шифрування SSL (Secure Sockets Layer), що гарантує, що дані які передаються між браузером користувача та серверами Google, залишаються в безпеці та зашифрованими. Підтвердженням цього є наявність в пошуковому рядку протоколу HTTPS https://….

Дане з'єднання є безпечним, та гарантує приватність та захищеність інформації, яка передається від браузера на сервер, що говорить про унеможливлення викрадення інформації під час передачі та запобігти хакерським

діям. Протокол SSL є доволі складним, але користувач під час роботи на сторінці браузера не помічає даної складності. Для встановлення SSL з'єднання на сервері необхідно встановлювати SSL сертифікат. [2]

Крім протоколу SSL Google Forms в стані спокою за замовчуванням, використовують протокол шифрування AES-256, для збереження даних на власних сервісах. Винятком є невелика кількість Persistent Disks, що були створені до 2015 року, для їх шифрування використовується AES-128 [3].

На сьогодні AES-256 є одним з найнадійніших алгоритмів шифрування. AES-256. AES-256 та AES-128 рекомендовані для тривалого зберігання даних Національним інститутом стандартів і технологій (NIST) [4].

Алгоритми AES шифрування являють собою симетричні блокові шифри за допомогою яких, здійснюється шифрування та дешифрування даних. Розмір ключа, який можна використати в AES дорівнює 128, 192 та 256 біт. За весь період існування алгоритму жодні дані, що були ним захищені не вдалося зламати. Оскільки, підбір можливих паролів розтягується при використанні AES 256 із 256 бітів, призводить до перебору 2^{256} можливих комбінацій. Така кількість варіантів робить метод перебору сильно часозатратний. На сьогодні не існує методів, які у прийнятний проміжок часу могли б зламати AES. Можливою загрозою для AES в майбутньому є квантові комп'ютери, але вони повинні бути досить потужними. Навіть за умови появи квантових комп'ютерів алгоритми шифрування AES залишаються досить надійними.

Аналогічні методи шифрування застосовуються і під час використання на пристроях Android та iOS.

2. Аналіз безпеки програмного забезпечення для адміністрування опитування Quizlet

Quizlet - багатонаціональна американська компанія заснована у 2007 році, яка надає інструменти для навчання. Основним наповненням Quizlet є цифрові флеш-картки, встановлення відповідностей, тести в режимі реального часу.

В розділі Політика конфіденційності Quizlet вказано, що Quizlet не продає особисту інформацію, отриману від дітей віком до 13 років (в деяких країнах відповідно місцевому законодавству до 16 років). В цей же час, Quizlet та сторонні рекламні партнери можуть відстежувати та показувати рекламу користувачам, коли вони відвідують сайт та можуть використовувати зібрану інформацію для надання релевантної реклами, що може становити потенційну загрозу для конфіденційності користувачів. Політика конфіденційності Quizlet запевняє, що їх веб-сервіс використовує шифрування даних та захищає їх загальноприйнятими стандартами. У відкритому доступі також відображається деяка інформація про користувача (наприклад, прізвище та ім'я автора тесту). При здійснені оплати для отримання додаткового функціоналу, Quizlet використовує сторонні платіжні процеси для здійснення управління платежами гарантуючи при цьому шифрування даних [5].

З політики конфіденційності стає зрозуміло, що Quizlet використовує шифрування даних, але які саме протоколи та криптоалгоритми використовуються не вказано. На початку пошукового рядка видно, що він

розпочинається з https://…, що може говорити про використання протоколу та сертифікату SSL, а також протоколу HTTPS, що як і в Google Forms дозволяє захистити дані під час здійснення обміну інформацією між браузером та серверами, але це являється лише базовим рівнем захисту інформації.

На сьогоднішній момент Quizlet не підтримує двофакторну аутентифікацію. Користувачам рекомендується для забезпечення захисту своїх персональних даних використовувати надійні паролі.

В майбутньому, планується розробити власну систему проведення тестувань. При цьому, буде взято до уваги методи передачі та зберігання даних, що описані вище. Зокрема шифрування даних в стані спокою за допомогою AES-256, розподіл контролю доступу користувачів на декілька рівнів з обмеженими правами. Для забезпечення академічної доброчесності буде реалізовано генерацію унікальних водяних знаків, які міститимуть закодовані дані про користувача. Це дозволить швидко визначати джерело витоку інформації та сприятиме підвищенню відповідальності серед учасників тестування.

Висновок. У процесі дослідження було здійснено аналіз забезпечення захисту інформації на платформах проведення опитування Google Forms та Quizlet, які використовуються найчастіше для проведення опитувань. Можна дійти висновку, що Google Forms забезпечують високу надійність даних, завдяки використанню SSL та AES-256 для обміну інформацією між клієнтом та сервером, а також її обміну, що надає захист даних у хмарі. Двофакторна аутентифікація, що підтримується Google Forms знижує ризики несанкціонованого доступу до акаунтів, що особливо важливо, якщо на них зберігається конфіденційна інформація. Quizlet використовує базові протоколи захисту, такі як SSL/HTTPS, не підтримує двофакторну аутентифікацію, що може становити потенційну загрозу для конфіденційних даних. В Quizlet згадується використання шифрування, проте конкретні протоколи та алгоритми не називаються, що залишає відкритим питання щодо забезпечення належного рівня захисту. Загалом, для створення та проведення конфіденційних опитувань Google Forms є більш надійним вибором, тоді як Quizlet підходить для неособистої та загальнодоступної інформації. Таким чином, вибір платформи для проведення опитування, має здійснюватися, з урахуванням необхідного рівня конфіденційності та цілісності даних, що використовуються під час опитування.

Перелік використаних джерел.

1. Google Forms. Безпека. [Електронний ресурс].- Режим доступу: https://www.google.com/intl/uk_ua/forms/about/#security

2. Are Google Forms secure? [Електронний ресурс].- Режим доступу: https://www.123formbuilder.com/blog/are-google-forms-secure

3. Default encryption at rest. [Електронний ресурс].- Режим доступу: https://cloud.google.com/docs/security/encryption/default-encryption

4. Transitioning the Use of Cryptographic Algorithms and Key Lengths. [Електронний ресурс].- Режим доступу: https://csrc.nist.gov/pubs/sp/800/131/a/r2/final

5. Політика конфіденційності Quizlet. [Електронний ресурс].- Режим доступу: https://quizlet.com/privacy