Секція 1

МЕТОД ЗАХИСТУ ПЛАТІЖНИХ ДАНИХ У ВЕБ-ЗАСТОСУНКУ ДЛЯ ОСББ

Волобуєва Д.М.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник: Землянко Г.А.

Актуальність. Сьогодні у світі є велика кількість різноманітних платіжних систем, завдяки чому все менше людей користуються готівковими розрахунками. Онлайн розрахунки спрощують життя людям за рахунок швидкості транзакцій, доступності з будь-якої точки світу за умови наявності інтернету, можливості проведення їх у будь-який час доби тощо. Вони використовуються у багатьох сферах, наприклад, таких як інтернет-покупки, оплата таксі тощо. Сфера ОСББ не стала виключенням. Для зручної оплати комунальних та житлових платежів через застосунки для ОСББ, необхідно використовувати платіжні системи.

Метою роботи є дослідження методів захисту платіжних даних.

Основні положення. Для початку необхідно визначити що є платіжною системою.

Платіжна система - платіжна організація, учасники платіжної системи та сукупність відносин, що виникають між ними при проведенні переказу коштів. Проведення переказу коштів є обов'язковою функцією, що має виконувати платіжна система [1]. До складу платіжної системи як екосистеми в цілому входить ціла низка учасників: платіжні провайдери, банки, центральний координуючий орган (як правило, центробанк країни), процесингові центри та провайдери технічної інфраструктури, що забезпечують обчислювально-комунікаційну базу для проведення платежів[2]. Усі учасники системи взаємодіють між собою за певними правилами та домовленостями, спираючись на чітко виписану законодавчу основу[2].

Існує основні два методи захисту інформації, що використовуються для захисту платіжної інформації найчастіше. Це токенізація та шифрування.

Шифрування – це засіб захисту цифрових даних за допомогою одного або декількох математичних прийомів, разом із паролем або «ключем», що використовується для дешифрування інформації. [3]. Існує два основних типи шифрування – це симетричне та асиметричне. При симетричному шифруванні використовується один ключ, як для шифрування, так і для дешифрування, що і є головною перевагою цього типу шифрування. За рахунок його простоти він є швидшим за асиметричний тип алгоритмів та потребує менше обчислювальних потужностей. При асиметричному шифруванні використовується два різних ключа. Одним з ключів може користатися хто завгодно, бо він є загальнодоступним і називається

«відкритим ключем». Другий ключ є приватним і називається «закритим ключем». Відкритий ключ використовується для шифрування даних, а закритий для дешифрування, що гарантує, що дані будуть розшифровані тільки особою, що має закритий ключ. Основною перевагою цього типу шифрування є підтримка роботи з неструктурованими базами даними.

Токенізація — це процес обміну конфіденційних даних на неконфіденційні дані, які називаються «токенами», які можна використовувати в базі даних або внутрішній системі, не зачіпаючи їх [4]. На відміну від шифрування, токенізація не використовує математичний процес для перетворення інформації. В процесі токенізації інформація замінюється на дані, які не мають цінності і їх неможливо використати у корисливих цілях. На відміну від зашифрованих даних, токенізовані нерозшифровуються і є незворотними.

Надійний захист платіжних даних також залежить від самих користувачів, тож окремо потрібно займатися освітою користувачів за допомогою інструктажів безпеки.

Висновки. В останні роки платіжні системи набули чималої популярності, через що, багато застосунків почали їх використовувати для зручного отримання оплати послуг. У сфері ОСББ онлайн платежі не стали виключенням. Додавання платіжної системи до застосунка дозволяє користувачам зручно сплачувати за комунальні та житлові послуги одразу з особового кабінету. Звісно постало питання захисту платіжних даних. Для зберігання платіжних даних найчастіше використовується токенізація та шифрування. Основним мінусом токенізації є складне масштабування для великих обсягів даних. Якщо хакери дізнаються ключ дешифрування, то дані будуть дешифровані, це і є основним мінусом шифрування. Для захисту даних найкраще використовувати токенізацію та шифрування разом.

Список літератури

1. Закон України Про платіжні системи та переказ коштів в Україні [ст. 1, п. 1.29]. URL: https://zakon.rada.gov.ua/laws/show/2346-14#Text (дата звернення: 07.11.22);
2. Що таке платіжна система та які з них працюють в Україні. *Fondy*. URL: https://fondy.ua/uk/knowledge/payment-system/ (дата звернення: 15.11.22);
3. Шифрування. *Nesrakonk*. URL: https://ua.nesrakonk.ru/encryption/ (дата звернення: 16.11.22);
4. What is Tokenization? *Tokenex*. URL: https://www.tokenex.com/blog/what-is-tokenization/ (дата звернення: 15.11.22);

Відомості про авторів

Волобуєва Дар'я Михайлівна, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 0999707472 d.volobueva@student.csn.khai.edu
Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки. g.zemlynko@csn.khai.edu