

ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ ОНЛАЙН ПЛАТЕЖІВ

Вінницький національний технічний університет

Анотація Досліджено систему захисту онлайн платежів на прикладі 3-D Secure. Базуючись на дослідженні, виявлено переваги та недоліки даного методу як зі сторони клієнта, так і зі сторони онлайн-магазину. Запропоновано способи покращення гарантії безпеки онлайн платежів.

Ключові слова: 3D-Secure, Visa, MasterCard, онлайн платежі, захист платежів.

Abstract An online payment protection system using 3-D Secure was investigated. Based on the research, the advantages and disadvantages of this method were identified, both from the client's side and from the online store's side. Ways to improve the security of online payments are suggested.

Keywords: 3D-Secure, Visa, MasterCard, online payments, payment protection.

Вступ

Життя в сучасному світі не можна уявити без онлайн-покупок та оплати рахунків в інтернеті, які роблять його легшим, але з приходом нових технологій з'являються нові шахраї, які готові забрати гроші собі. Для гарантії безпеки і захисту персональних даних користувача було розроблено унікальну технологію 3D-Secure, на яку покладаються задачі забезпечення безпеки при взаємодії клієнт-банк-продавець [1].

Метою є покращення безпеки при здійсненні платежів внаслідок дослідження відомої технології 3D-Secure.

Результати дослідження

Основними задачами при онлайн оплаті є забезпечення гарантії захисту транзакції та персональних даних користувача.

Технології VerifiedbyVisa [2] і SecureCode [3] найкраще захищають не банки, а саме інтернет-магазини. Якщо банк-емітент схвалює транзакцію в магазині, де діє правило введення додаткового коду, то він бере на себе відповідальність за легітимність операції. Банк, схваливши платіж, не має права вимагати назад гроші у продавця. Якщо картка покупця підключена до послуги 3D-Secure, то банк має можливість запросити у клієнта додатковий пароль і зайвий раз переконатися в тому, що платник – справжній власник. Якщо послугу банк не увімкнув, то відповідальність лягає на нього і може захищатися лише найпростішим способом – забороняючи платіжну операцію на сайті, де він позбавлений можливості проводити chargeback.

Аутентифікація 3D-Secure заснована на трьох незалежних доменах: еквайра (банк, що обслуговує інтернет-магазин), емітента (банк, що приймає оплату від власників платіжних карток за товари чи послуги), сумісності (домен відповідної платіжної системи).

Головна перевага VerifiedbyVisa і SecureCode в тому, що в процесі здійснення транзакції через Інтернет клієнту необхідно вводити пароль, що підтверджує транзакцію. Його можна отримати у вигляді СМС-повідомлення, що забезпечує гарантію безпеки, тому що здійснюється розділення каналів зв'язку. На відміну від використання токена операції, який може бути перехоплено і підмінено.

Кожен з доменів виконує строго відведену роль: емітент відповідає за надання правильної інформації про клієнта, еквайр - за коректний запит і правильний шлях перенаправлення власника карти, платіжна система - за збереження даних.

Спрощена схема проведення онлайн платежу зображена на рисунку 1. Після запиту на оплату товару або послуги сервер інтернет-магазину посилає запит на підтвердження операції, в цей час сервер контролю доступу, банка-емітента, надсилає код підтвердження (СМС-повідомлення) клієнту для підтвердження його особи. Після підтвердження операції банк-емітент здійснює переказ коштів банку-еквайру.

Технологія 3D-Secure є унікальною і утримує ціни на високому рівні. У будь-якого банку є кілька можливостей для того, щоб почати надавати своїм клієнтам послуги 3D-Secure – можна реалізувати це за допомогою залучення зовнішньої компанії або власними силами.

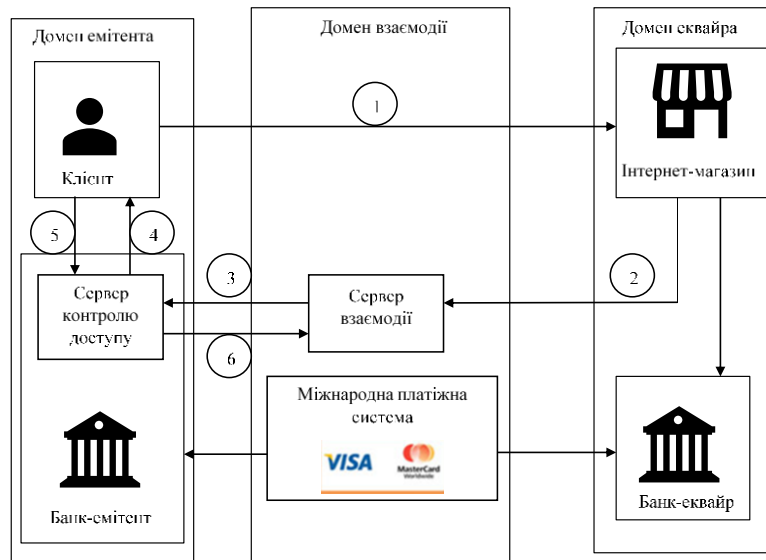


Рисунок 1 – Схема проведення онлайн платежу

Такий спосіб під силу лише багатим і досить великим структурам. Вибір зовнішньої організації як постачальника послуги дозволяє уникнути деяких технічних проблем.

Доцільність підключення додаткового підтвердження онлайн-операцій по карті залежить від того, як часто клієнти банку використовують свої карти для здійснення подібних транзакцій. Зрозуміло, що для провідних роздрібних банків, зацікавлених у збільшенні обсягів безготівкових операцій по картах, питання впровадження технології 3D-Secure досить важливе.

Перевагами 3D-Secure є: гарантована безпека, простота, зручність, основним недоліком – якщо картка підключена до 3D-Secure, але інтернет-сайт не підтримує технологію 3D-Secure, то операція здійснюється в стандартному режимі (без введення одноразового пароля, але з використанням лімітів для карток з 3D-Secure).

Висновки

Розглянуто основні переваги та недоліки технології 3D-Secure та доцільність її використання для банків та інтернет-магазинів. Унаслідок дослідження буде реалізовано програмний модуль, що використовує технологію захищених платежів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. EMV® 3-D Secure [Електронний ресурс]: [Веб-сайт]. – Режим доступу:URL: <https://www.emvco.com/emv-technologies/3d-secure/>, вільний – Назва з екрана.
2. Strong Customer Authentication [Електронний ресурс]: [Веб-сайт]. – Режим доступу:URL: <https://www.visa.co.uk/pay-with-visa/changes-in-payment-security.html>, вільний – Назва з екрана.
3. Mastercard Anti-Piracy Polic [Електронний ресурс]: [Веб-сайт]. – Режим доступу:URL: <https://www.mastercard.us/en-us/about-mastercard/what-we-do/anti-piracy-policy.html>, вільний – Назва з екрана.

Звіряка Лілія Олександрівна – студент, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: lzviryaka333@gmail.com

Науковий керівник: **Войтович Олеся Петрівна** – канд. техн. наук, доц., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Zviryaka Liliia O. – student, Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: lzviryaka333@gmail.com

Supervisor: **Voitovych Olesia P.** – PhD, Cand. of Tech. Sc., Assistant Professor of Information Protection department, Vinnytsia National Technical University, Vinnytsia