 ISSN 2226-3780

УДК 338.24; 343.5; 005.3; 004.8
DOI: 10.15587/2312-8372.2015.41739

Йона О. О.

ДОСЛІДЖЕННЯ СТАНУ СУЧАСНИХ ТЕХНОЛОГІЙ ЗАХИСТУ ЕЛЕКТРОННИХ ТРАНЗАКЦІЙ

У статті розглядаються сучасні технології захисту електронних транзакцій в платіжних системах, зокрема, рішення на базі технологій SET и 3-D Secure. Розглянуті переваги та недоліки наданих технологій та зроблені висновки щодо стану сучасних протоколів захисту електронних транзакцій.

Ключові слова: *захист електронних транзакцій в платіжних системах, технологія SET, технологія 3-D Secure.*

1. Вступ

Розвиток технологій електронних платежів потребує використання сучасних методів захисту електронних транзакцій в платіжних системах. Технології захисту інформації також стрімко розвиваються, тому є необхідність подальшого дослідження цього питання з метою удосконалення протоколів захисту під час Інтернет еквайрингу [1–4].

Інтернет еквайринг – процес здійснення платежів при використанні пластикової картки через мережу Інтернет. При цьому картка має бути такою, щоб її власник мав змогу розраховуватись нею і в звичайних магазинах.

Транзакція – це банківська операція, що полягає в переказі грошових коштів з одного рахунку на інший чи видачі готівки в банкоматах та банківських установах.

Електронна пластикова картка – це є платіжний інструмент, що дає змогу його власнику виконувати безготівковий платіж за товар чи послугу, а також отримання готівки в банкоматах та банківських установах.

Електронна платіжна система – це є система, де в якості платіжного інструменту використовуються пластикові картки.

Платіжні системи можуть здійснювати операції як за допомогою готівки, так і безготівковими засобами.

Існує багато різних електронних платіжних систем, серед них Visa, MasterCard, EasyPay, Portmone, iPay та інші. Проте не можна назвати систему, яка б домінувала в різних напрямках, тому готівки та кредитні картки використовуються разом з електронними аналогами. В Україні найпоширенішими є системи Visa та MasterCard. Корпорації Visa та MasterCard постійно розробляють інноваційні рішення на основі даних і аналітичних висновків, щоб підвищити безпеку і захищеність електронних платежів. У статті аналізуються сучасні технології захисту електронних транзакцій в платіжних системах, зокрема, рішення на базі технологій SET и 3-D Secure, які були розроблені платіжними системами Visa і MasterCard.

2. Аналіз літературних даних та постановка проблеми

Проблемам дослідження методів захисту інформації в електронних платіжних системах присвячені праці багатьох вчених, включаючи зазначених в [1–12]. Так, у [1] класифікуються за призначенням методи криптографічного захисту документообігу. У [2] розглянута проблема забезпечення безпеки електронних платежів. Проблемам дослідження методів захисту інформації в локальних мережах банку присвячено [3]. Питання забезпечення безпеки інформації при використанні пластикових карток за допомогою технології 3-D Secure обговорюються в [4]. У [5] розглядається розподілена система виявлення шахрайських платежів. Протокол захисту електронних платежів 3-D Secure описується у [6]. Сучасні принципи побудови захищених інтелектуальних мереж, які можуть використовуватися у системах забезпечення економічної безпеки та організація процесу розробки програмного забезпечення для них, розглядаються у [7]. У [8] відзначені специфічні чинники, які підсилюють активізацію загроз економічній безпеці господарюючих суб'єктів. У [9] зроблена систематизація типових моделей загроз безпеці персональних даних, які обробляються в спеціальних інформаційних системах підприємств. У [10] розглянуто новий предмет інформаційних правовідносин – відомості щодо наданих людині телекомунікаційних послуг, які водночас опрацьовано в ролі предмета інформаційної безпеки людини як споживача телекомунікаційних послуг. Запропоновано нову модель забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг. У [11] описуються кібер стандарти безпеки і промислового застосування: системи та методології. У [12] розглядаються принципи, методи та програми ситуаційної обізнаності в комп'ютерній мережі, що захищається. Проте, в вищезазначених роботах не дається аналіз сучасних технологій захисту, тому можна зробити висновок про необхідність подальшого вивчення і удосконалення технологій захисту електронних транзакцій в платіжних системах.

3. Об'єкт, ціль та задачі дослідження

Об'єктом дослідження є сучасні технології захисту електронних транзакцій в платіжних системах, зокрема, рішення на базі технологій SET и 3-D Secure.

Метою дослідження є визначення стану сучасних технологій захисту електронних транзакцій під час інтернет еквайрингу.

Для досягнення поставленої мети необхідно виконати такі задачі:

1. Порівняти технології захисту електронних платіжних систем SET і 3-D Secure.

2. Визначити переваги та недоліки сучасних технологій захисту електронних транзакцій.

3. Зробити висновки щодо стану технологій захисту електронних транзакцій.

4. Результати дослідження стану технологій захисту електронних транзакцій

Для захисту електронних транзакцій під час інтернет еквайрингу необхідно використовувати надійні механізми захисту електронних платіжних систем. Саме з цією метою використовуються сучасні криптографічні протоколи захисту інформації (шифрування, розподілення ключів та автентифікацію) [1].

Одним з таких протоколів є технологія SET (Secure Electronic Transactions) «Безпечні електронні транзакції», розроблена платіжними системами Visa і MasterCard. У цьому протоколі для захисту транзакцій при здійсненні електронних платежів використовуються процедури шифрування і цифрового підпису. Протокол гарантує, що при взаємодії власника пластикової карти і продавця, інформація про рахунок кредитної карти залишатиметься конфіденційною (використовується подвійний цифровий підпис) [4–8].

Існує дві схеми використання протоколу SET.

У першій схемі використовуються відкриті ключі, при цьому кожен крок реалізації протоколу SET супроводжується автентифікацією. Це не дає можливості зловмисникові стати посередником і видозмінювати ці транзакції. Для нормальної роботи протоколу SET усі учасники повинні зареєструватися і передати партнерам свій відкритий ключ.

У другій схемі ідентифікація сторін робиться шляхом обміну цифровими сертифікатами, які засвідчують право учасників угоди використовувати пластикові карти. При цьому SET-сертифікат магазину містить ідентифікаційні параметри торгової точки. SET-сертифікат власника карти несе інформацію, яка має бути зашифрованою про основні параметри карти. Проведення оплати з використанням SET-сертифікату не вимагає від клієнта введення параметрів його карти і не передбачає отримання продавцем цієї конфіденційної інформації.

Система також дозволяє здійснювати платежі за допомогою пластикових карт і без використання SET-сертифікатів клієнта, у разі, якщо клієнти таких сертифікатів не мають. В цьому випадку використовується технологія MIA SET (Merchant Initiated Authorization). Для забезпечення безпеки платежів за технологією MIA SET, платіжна система запобігає можливим шахрайським транзакціям.

Перевагою протоколу SET є повна конфіденційність угоди, проте головним недоліком залишається велика вартість впровадження цієї технології і дорожнеча у використанні. Крім того, рівень шахрайства в мережі доки дозволяє користуватися доступнішими протоколами.

Корпорація VISA розробила протокол 3-D Secure з метою підвищення рівня безпеки електронних платежів і запропонувала клієнтам послугу Verified by Visa (VbV). Послуги, ґрунтовані на цьому протоколі, також були прийняті MasterCard під назвою MasterCard SecureCode (MCC) і JCB International як J/Secure.

Сучасний протокол 3-D Secure позбавлений недоліків протоколу SET, які заважають його впровадженню, а саме: він дешевше в реалізації, зручніше у використанні і додає ще один крок автентифікації при здійсненні електронних платежів.

Протокол 3-D Secure дозволяє додати до процесу фінансової авторизації перевірку достовірності в режимі реального часу. Ця автентифікація ґрунтується на принципі трьох доменів (звідси 3-D в назві):

– домен еквайєра (домен продавця і банку, в який перераховуються гроші);

– домен емітента (домен власника картки і банка, що видав картку);

– домен сумісності (домен, що надається платіжною системою (MasterCard, Visa, CyberPlat і т. д.) для підтримки протоколу 3-D Secure).

При цьому кожен з доменів виконує свою функцію:

– еквайєр відповідає за коректний запит і вірний шлях перенаправлення власника карти;

– емітент відповідає за надання достовірної інформації про клієнта;

– платіжна система відповідає за збереження даних.

При здійсненні платежу картою банку, що підтримує протокол 3-D Secure, до необхідної інформації додається додатковий запит на підтвердження дійсності карти (звичайно це одноразовий пароль підтвердження, який надсилається банком в SMS-повідомленні на мобільний телефон клієнта).

Доставка одноразового пароля за допомогою SMS, напевно, найпростіший спосіб надання коду для підтвердження операції. Передбачається, що, якщо клієнт ввів одноразовий пароль, у нього на руках є мобільний телефон з SIM-картою, зареєстрованою в інтернет-банку.

Проте, існує безліч способів обходу такого захисту. Усе більш популярним стає перехоплення управління смартфоном за допомогою мобільної троянської програми. Якщо шахраєві відомі данні платіжної картки, мобільний троян, що заразив пристрій може пересилати йому SMS-повідомлення з кодами підтвердження, щоб той міг використати їх для переказу грошей. Проте недоліком такого методу передачі коду підтвердження є затримка самого SMS-повідомлення. Тому для захисту від злочину використовується допустимий час затримки SMS-повідомлення.

Деякі банки використовують систему постійних паролів (отриманих при реєстрації) і при здійсненні кожної електронної транзакції клієнт вводить саме його. Проте такий спосіб автентифікації є менш надійним, чим одноразовий пароль підтвердження.

У технології захисту 3-D Secure також є такі недоліки. В звичайних транзакціях відповідальність за операції по вкрадених картах несе підприємство, на сайті якого була зроблена купівля товару чи послуги

за допомогою вкраденої карти (за умови, що він не підтримує технологію 3-D Secure). У разі ж транзакцій, які захищаються за технологією 3-D Secure, відбувається так зване «Перенесення відповідальності» (англ. Liability Shift), коли відповідальність переноситься на банк-емітент, що випустив карту, або на самого клієнта.

Проте головним недоліком технології 3-D Secure є те, що для захисту конфіденційної інформації використовується криптографічний протокол SSL/TLS (розробку протоколу SSL здійснювала компанія *Netscape Communications* для додання протоколу HTTPS до свого веб-браузеру Netscape Navigator. Надалі, на підставі протокола SSL 3.0 було прийнято стандарт RFC, якому дали ім'я протоколу TLS), який має багато вразливостей [4].

5. Обговорення результатів дослідження стану технологій захисту електронних транзакцій

Дослідження стану технологій захисту електронних транзакцій дає змогу визначити переваги та недоліки сучасних технологій захисту електронних транзакцій. Рівень шахрайства в мережі доки дозволяє користуватися протоколами, які мають вразливості. Оскільки шахрайські методи здобуття інформації під час інтернет еквайрингу нестримно розвиваються, проте виникає необхідність виявлення вразливостей сучасних протоколів захисту та подальшого дослідження, що дає змогу їхнього удосконалення.

Усунення виявлених недоліків підвищить безпеку транзакцій під час інтернет еквайрингу.

Проведений аналіз стану технологій захисту електронних транзакцій показав про необхідність подальшого дослідження і удосконалення технологій захисту електронних транзакцій в платіжних системах під час інтернет еквайрингу.

6. Висновки

В результаті проведених досліджень:

1. Зроблено аналіз та порівняння технологій захисту електронних платіжних систем SET і 3-D Secure, що дає змогу визначити їх основні переваги та недоліки.

2. Визначено переваги та недоліки сучасних технологій захисту електронних транзакцій. Перевагою технології SET є повна конфіденційність угоди, а недоліками є висока вартість впровадження і складність використання цього протоколу захисту. До переваг технології 3-D Secure можна віднести невисоку вартість реалізації і простоту використання. Проте, в технології 3-D Secure є свої недоліки. Це, в першу чергу, використання уразливого криптографічного протоколу SSL/TLS, хоча він «підсилюється» додатковим кроком автентифікації і в другу – «перенесення відповідальності» на самого клієнта (чи на банк-емітент), у разі використання зловмисником вкраденої карти. А якщо зловмисник разом з карткою клієнта може використовувати ще й мобільний телефон клієнта, то здійсненню шахрайського платежу практично нічого не завадить.

3. Підводячи підсумок, можна зробити висновок про необхідність подальшого вивчення і удосконалення технологій захисту електронних транзакцій в платіжних системах.

Література

1. Йона, Л. Г. Криптографічний захист електронного документообігу [Текст] / Л. Г. Йона, О. О. Йона, В. С. Терешко // Цифрові технології. – 2013. – № 13. – С. 142-146.
2. Балакирский, В. Б. Безопасность электронных платежей [Текст] / В. Б. Балакирский // Конфидент. – 1996. – № 5. – С. 47-53.
3. Гайкович, В. Ю. Безопасность электронных банковских систем [Текст]: учебник / В. Ю. Гайкович, А. С. Першин. – М.: Единая Европа, 1994. – 354 с.
4. Быхно, А. 3D-Secure: безопасные покупки через Интернет [Электронный ресурс] / Александр Быхно. – Режим доступа: \www/URL: http://credit-card.ru/articles/security/3d-secure.php
5. Фахретдинов, Р. Анализ средств подтверждения банковских транзакций [Электронный ресурс] / Руслан Фахретдинов. – Режим доступа: \www/URL: http://frodex.ru/article/authentification2014
6. 3-D Secure [Электронный ресурс]. – Режим доступа: \www/URL: http://www.bankdbo.ru/3-d-secure
7. Гончаров, В. В. Безопасность и защита интернет-платежей [Электронный ресурс] / В. В. Гончаров // Расчеты и операционная работа в коммерческом банке. – 2010. – № 4. – Режим доступа: \www/URL: http://bankir.ru/tehnologii/s/bezopasnost-i-zaschita-internet-platejei-5899180/
8. Йона, О. О. Специфічні чинники активізації загроз економічній безпеці господарюючих суб'єктів [Текст] / О. О. Йона // Технологічний аудит та резерви виробництва. – 2012. – № 4/6 (8). – С. 31-32. – Режим доступу: http://journals.uran.ua/tarp/article/view/5645
9. Йона, О. О. Огляд та систематизація типових моделей загроз безпеці персональних даних, які обробляються в спеціальних інформаційних системах підприємств [Текст] / О. О. Йона // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2012. – № 8 (179), Ч. 1. – С. 110-117.
10. Арістова, І. В. Інформаційна безпека людини як споживача телекомунікаційних послуг [Текст]: монографія / І. В. Арістова, Д. В. Сулацький. – К.: Ред. журн. «Право України»; Х.: Право, 2013. – 184 с.
11. Junaid Ahmed Zubairi. Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies [Text] / Junaid Ahmed Zubairi, Athar Mahboob. – IGI Global, 2011. – 336 p. doi:10.4018/978-1-60960-851-4
12. Cyril Onwubiko. Situational Awareness in Computer Network Defense: Principles, Methods and Applications [Text] / Cyril Onwubiko, Thomas Owens. – IGI Global, 2012. – 414 p. doi:10.4018/978-1-46660-104-8

ИССЛЕДОВАНИЕ СОСТОЯНИЯ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ЗАЩИТЫ ЭЛЕКТРОННЫХ ТРАНЗАКЦИЙ

В статье рассматриваются современные технологии защиты электронных транзакций в платежных системах, в частности, решения на базе технологий SET и 3-D Secure. Рассмотрены преимущества и недостатки данных технологий защиты и сделаны выводы относительно состояния современных протоколов защиты электронных транзакций.

Ключевые слова: защита электронных транзакций в платежных системах, технология SET, технология 3-D Secure.

Йона Олена Олегівна, *викладач, здобувач, кафедра інформаційних систем в економіці, Одеський національний економічний університет, Україна,* ***e-mail: eyona@mail.ru****.*

Йона Елена Олеговна, *преподаватель, соискатель, кафедра информационных систем в экономике, Одесский национальный экономический университет, Украина.*

Yona Olena, *Odessa National Economic University, Ukraine,* ***e-mail: eyona@mail.ru***