МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01ммзи
_____ Жачко А.Н.
(подпись)

Отчет защищен с оценкой

_____

_____ С.С. Зотов
(подпись) (И.О. Фамилия)

« 31 » июля 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН

_____ С.С. Зотов
(подпись) (И.О. Фамилия)

Регистрационный № _____
« 31 » июля 2021 г.

_____ Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.
на предприятии
Кафедра информационной безопасности ШЕН ДВФУ

г. Владивосток
2021

Содержание

Задание на практику

- Проведение исследования в области безопасности современных платёжных технологий
- Написание отчета по практике о проделанной работе.
- Написание тезисов по выбранной теме.
- Подготовка презентации по проведённому исследованию.

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 19 июля 2021 года по 31 июля 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1. Ознакомиться с используемыми типами платёжных систем и их классификацией.
2. Изучить принципы их работы и алгоритмы, используемые для их защиты.
3. На основе полученных знаний написать отчет по практике о проделанной работе.

Безопасность современных платёжных технологий

Несмотря на то, что наиболее популярным способом совершения транзакций в мире до сих пор являются наличные платежи, процент использования электронных платёжных систем неумолимо растёт. Помимо непосредственного удобства, возможность управлять своими средствами дистанционно стала намного актуальнее в реалиях пандемии COVID-19. Такая возможность стала доступна рядовым клиентам банков благодаря внедрению информационных технологий в процессы совершения экономического взаимодействия. Совершение транзакций посредством платёжных систем гарантирует отсутствие необходимости в непосредственном контакте плательщика и получателя платежа, что, при повсеместном внедрении улучшает санитарно-эпидемиологическую обстановку. Кроме повышения уровня личной безопасности в рамках пандемии, к преимуществам электронных платежей можно отнести высокую скорость операций, низкую стоимость каждой операции, а также облегчение процесса трансграничных платежей.

В наше время есть несколько факторов, стимулирующих развитие электронных платёжных технологий. С точки зрения социально-экономических условий таковым является отсутствие альтернатив наличным платежам, которое способствует увеличению пользователей, предпочитающих электронные платежи. Также значимым фактором является экономическая эффективность: большинство онлайн-транзакций имеют низкую стоимость при значительном объёме. К примеру, комиссия за отправку денег за рубеж с помощью системы MTN составляем 0.05 доллара США, а средняя стоимость доставки наличных – от 30 до 50 долларов США. Кроме того, сейчас многие неправительственные организации предлагают инициативы по поощрению внедрения платёжных технологий повсеместно. В противовес этим факторам, существуют также ограничители развития

электронных платёжных технологий. К таковым относятся давление банков, ограниченное сотрудничество с этими системами, слаборазвитая инфраструктура систем, а также, что первостепенно, проблемы с безопасностью.

В общем случае процесс совершения электронной транзакции состоит из пяти основных звеньев: эмитент, эквайер, клиент, продавец и платёжный шлюз, являющийся средой, которая объединяет четыре стороны. Весь процесс можно описать в семь шагов:

1. Клиент отправляет запрос на совершение операции продавцу.
2. Продавец запрашивает у платёжного шлюза депозит в размере суммы транзакции.
3. Клиент отправляет запрос на платёжный шлюз для проверки суммы списания.
4. В платёжном шлюзе осуществляется оформление платежа.
5. Платёжный шлюз отклоняет/одобряет запрос клиента.
6. Платёжный шлюз отклоняет/одобряет запрос продавца.
7. Продавец подтверждает транзакцию и предоставляет клиенту квитанцию об оплате.

В России с февраля 2013 года принята следующая классификация электронных платёжных систем: дистанционные финансовые сервисы, интернет-платежи, терминалы и эквайринг. Первая категория включает в себя сервисы мобильных платежей и интернет-банкинг, к первому относятся мобильный банкинг, SMS-банкинг (служба коротких сообщений), мобильные операторские платежи и NFC-платежи, а ко второму небанковские немобильные сервисы или системы электронных денег. Интернет-платежные системы различаются по видам оплаты на карточные, операторы цифровой наличности и платёжные шлюзы. Карточные платёжные системы – системы,

в которых оплата производится на сайте продавца с помощью банковской карты. В случае операторов цифровой наличности оплата производится посредством электронных денег или цифровой наличности, то есть некой внутренней валюты, которую можно обналичить у соответствующих участников электронных платёжных систем. Платёжные шлюзы, в свою очередь, представляют собой объединение предыдущих двух категорий. Важно отметить, что именно к шлюзам относится значительная часть существующих систем.

Говоря простым языком, любая платёжная система является способом осуществлять финансовые транзакции с помощью банковских карт или электронной наличности, то есть без использования наличных денег. Эти системы совершенствуются пропорционально развитию информационных технологий, что делает их всё более разумной альтернативой наличным платежам. Сейчас существует множество платёжных систем, каждая из которых имеет свои достоинства и недостатки, однако одной из наиболее сложных задач в этой сфере является оценка безопасности. По данным MasterCard от 2013 года, объёмы мошенничества в электронных платёжных системах в три раза превышают аналогичные при наличии карты.

Гарантией того, что та или иная платёжная система может считаться надёжной, в том числе с точки зрения защиты информации пользователей, служат семь основных условий:

1. Конфиденциальность. Данные пользователей должны быть защищены от ознакомление с её содержанием лиц, не имеющих права доступа к ней. В большинстве современных платёжных систем конфиденциальность обеспечивается криптографическими средствами.
2. Целостность информации. Гарантирование невозможности несанкционированного изменения информации. Для обеспечивания

этого условия необходим некий критерий обнаружения манипуляций. Обычно в этих целях используются хэш-функции.

3. Аутентификация. Подтверждение подлинности сторон и самих данных в процессе взаимодействия. Взаимная аутентификация пользователей обеспечивается с помощью ключей ассиметричного шифрования, пароля и номера учётной записи.
4. Авторизация. Проверка готовности пользователя к взаимодействию.
5. Выбор средств оплаты. Пользователь имеет возможность совершить транзакцию любыми денежными средствами, которые ему доступны.
6. Гарантия рисков. Поставщик услуг должен публиковать пользователю перечень задокументированных рисков, и предоставлять гарантии от них.
7. Минимизация оплаты транзакций. Оплата обработки запроса представляет собой комиссию от платежа, которая, по возможности, должна быть минимизирована.

Однако, ни одна из существующих сейчас платёжных систем не отвечает всем этим требованиям в полной мере, поэтому в каждом случае может быть сформулирован конкретный список требований к безопасности. Помимо непосредственно архитектуры системы, дополнительным уровнем защиты информации в системах электронных платежей служат криптографические протоколы.

Одним из наиболее популярных протоколов обеспечения безопасности платёжных систем является протокол 3-D Secure, который используется в качестве дополнительного уровня безопасности для онлайн-карт и двухфакторной аутентификации пользователей, однако не гарантирует безопасность денежных средств. Изначально технология была разработана как средство повышения уровня безопасности интернет-платежей для

платёжной системы Visa, однако позже была принята системами MasterCard, JCB International, AmEx и Мир. Протокол добавляет в онлайн-платежи ещё один шаг аутентификации, который позволяет поставщикам услуг дополнительно убедиться в личности держателя карты. Для этого используется одноразовый код, который передаётся пользователю и требуется для подтверждения факта владения картой. Это значительно сокращает число возможных мошеннических операций, однако не является гарантией полной безопасности. Риск перехвата одноразового кода является значительной уязвимостью данного протокола. Важно упомянуть, что при совершении транзакции без дополнительного шага аутентификации возможен так называемый «Перенос ответственности» (Liability Shift), то есть потенциальная возможность пользователя вернуть свои средства при своевременном обращении.

Так же стоит отметить стандарт EMV (Europay + MasterCard + VISA) – международный стандарта, разработанный с целью повышения уровня безопасности финансовых операций с контактными и бесконтактными картами. В стандарте определяются физическое, электронное и информационное взаимодействие между терминалом и, непосредственно, картой. Выпуск карт, удовлетворяющих данному стандарту, начался в 2010 года в США, и на сегодняшний день не обнаружены уязвимости данного стандарта в случае с чиповыми картами. Однако при совершении транзакций без использования чипа уязвимость возрастает.

Руководитель департамента управления рисками Visa в России, Эвелина Нечипоренко, в конце 2020 года выступила с прогнозами на ближайшие несколько лет. По её мнению, опыт пандемии позволит увеличить темпы внедрения цифровых платежей, а также даст серьёзный толчок их совершенствованию. По данным Visa, использование бесконтактных карт выросло на 41%, мобильных платежей – на 31%, а также большую популярность получили покупки онлайн. В связи с резким ростом

использования платёжных систем, выросла и необходимость повысить их безопасность. Таким образом, значительная часть участников платёжного рынка заинтересована в модернизации платёжной инфраструктуры.

Анализ различных источников даёт возможность сделать вывод, что актуальность вопросов безопасности современных платёжных технологии будет расти в связи с повышением популярности электронной коммерции в мире. Для того, чтобы своевременно удовлетворять нужды потребителей, финансовые организации продолжат вкладывать ресурсы в развитие платёжных систем. Однако фундаментальной задачей остаётся обеспечение безопасности электронных платежей, что предполагает постоянное обновление стратегий защиты средств как пользователей, так и организаций.

Заключение

Для достижения данной цели, в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики ознакомилась с используемыми в наше время платёжными системами, с принципами их работа, а также с методами, которые используются для обеспечения их безопасности.

Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

Список используемых источников

1. WAQAS AHMED, AAMIR RASOOL, ABDUL REHMAN JAVED, NEERAJ KUMAR, THIPPA REDDY GADEKALLU, ZUNERA JALIL, NATALIA KRYVINSKA – « Security in Next Generation Mobile Payment Systems: A Comprehensive Survey»
2. S. EDITION – «Cryptography and network security»
3. [Электронный ресурс]. - https://www.visa.com.ru
4. [Электронный ресурс]. -https://www.mastercard.us/en-us.html
5. Семенов Ю.А. (ИТЭФ-МФТИ) - «Телекоммуникационные технологии»