Список использованной литературы

1. Аношкин А.П. Педагогическое проектирование систем и технологий обучения: учеб. пособие [Текст]/ А.П. Аношкин. - Омск, Изд-во ОмГПУ,1997. – 138 с.

2. Кораблёв А. А. Информационно-телекоммуникационные технологии в образовательном процессе[Текст]/А.А. Кораблев // Школа. – 2006. - №2. – С.37-39.

3. Петухова Е.И. Информационные технологии в образовании[Текст]/Е.И. Петухова // Успехи современного естествознания. – 2013. – № 10. – С.80-81.

4. Сластенин В. А., др. Педагогика: учеб. пособие для студ. высш. пед. учеб. Заведений / под ред. В. А. Сластенина. М.: Издательский центр «Академия», 2002. 576 с.

5. Тевс Д. П., Подковырова В. Н. Использование современных информационных и коммуникационных технологий в учебном процессе: учебно-методическое пособие / авторы-составители: Д. П. Тевс, В. Н. Подковырова, Е. И. Апольских, М. В. Афонина. Барнаул: БГПУ, 2006. 45 с.

Электронные ресурсы:

I. Справочник по педагогике [Электронный ресурс] /Электронные текстовые данные. Режим доступа: https://spravochnick.ru/pedagogika/informacionno-communikacionnye_tehnologii/

Галисултанов Руслан Ирмухаметович
ФГБОУ ВО «Курганский государственный университет»,
студент кафедры «Безопасность информационных и автоматизированных систем»,
galisultanov98@gmail.com, Курган, Россия
Москвин Владимир Викторович
ФГБОУ ВО «Курганский государственный университет»,
старший преподаватель кафедры
«Безопасность информационных и автоматизированных систем»,
bias@kgsu.ru, Курган, Россия
Человечкова Анна Владимировна
ФГБОУ ВО «Курганский государственный университет»,
старший преподаватель кафедры
«Безопасность информационных и автоматизированных систем»,
chelovechkova_2011@mail.ru, Курган, Россия

БЕЗОПАСНОСТЬ БЕСКОНТАКТНОЙ ОПЛАТЫ

УДК 004.056:336.717

Аннотация. За последние пять лет в Российской Федерации, как и во всем мире, широкое распространение получила технология бесконтактной оплаты, что закономерно: она упрощает процесс оплаты, позволяя использовать для этих целей носимые устройства, такие как смарт-часы или смартфон вместо традиционной оплаты пластиковой картой. При этом многие задаются вопросом: насколько безопасно ее использование? В данной статье рассматриваются виды систем совершения бесконтактных платежей, их особенности и безопасность

Ключевые слова: бесконтактная оплата, NFC, токены, безопасность информации.

Abstract. Over the past five years in the Russian Federation, as well as throughout the world, contactless payment technology has become widespread, which is natural: it simplifies the payment process by allowing the use of wearable devices, such as a smart watch or smartphone, for these purposes instead of the traditional payment with a plastic card. At the same time, many ask the question: how safe is its use? This article discusses the types of contactless payment systems, their features and security.

Keywords: contactless payment, NFC, tokens, information security

Две трети потребителей считают бесконтактные платежи безопасными. Об этом свидетельствуют результаты исследования, проведенного Аналитическим центром Национального агентства финансовых исследований в феврале 2020 года [1]. Банковские карты являются сегодня распространенным платежным средством: подавляющее большинство россиян (82 %) – держатели банковских карт, причем за последние 11 лет их доля выросла с 31 % до 82 %.

Большинство россиян знают о возможности оплачивать товары и услуги путем бесконтактных платежей с помощью банковской карты (93 %) или мобильного телефона (88 %). В меньшей степени осведомлены о платежах с других устройств – смартчасов и браслетов (65 %).

Значительная часть россиян – 60 % – оплачивают свои покупки бесконтактным способом. Так, более половины (58 %) использовали для бесконтактной оплаты банковские карты. Каждый четвертый (26 %) платил за

товары или услуги при помощи смартфона, причем за год число тех, кто использовал этот метод, выросло на 15 процентов. 7 % использовали для оплаты смартчасы или браслеты.

Те, кто платил электронными устройствами, чаще всего осуществляли оплату при помощи сервиса Google Pay (44 %), на втором месте – Apple Pay (33 %), на третьем – Samsung Pay (11 %).

Россияне считают технологию бесконтактной оплаты удобной. Те, кто знаком с технологией бесконтактной оплаты, чаще отмечали удобство платежей посредством банковской карты (80 %) и смартфона (70 %). Многие говорят, что оплату товаров и услуг удобно осуществлять при помощи смартчасов (63 %), браслетов (60 %) и брелоков (56 %).

При этом треть опрошенных считают, что бесконтактные формы оплаты не являются безопасными. Далее в таблице приведены данные о количестве тех, кто считает различные способы бесконтактной оплаты небезопасными [1].

Способы бесконтактной оплаты

	% тех, кто считает технологию небезопасной
Бесконтактная оплата банковской картой	30
Бесконтактная оплата с помощью смартфона	32
Бесконтактная оплата с помощью наручных часов	33
Бесконтактная оплата с помощью специального наручного браслета	33
Бесконтактная оплата с помощью специального брелока	36

Обоснованы ли сомнения данной группы пользователей относительно данной технологи?

Разумеется, в сравнении, например, с банковской картой, обладающей только контактным способом оплаты – обычно магнитная полоса и/или микропроцессор, пластиковая карта, поддерживающая возможность бесконтактного платежа более уязвима [2]. Рассмотрим этот вопрос подробнее.

Большинство переживаний простых пользователей связаны с возможностью без подтверждения ПИН-кодом проводить так называемые

микротранзакции – платежи, сумма которых обычно не превышает 1000 рублей. Отметим, что в 2019 году международная платежная система VISA увеличила лимит на совершение микротранзакций до 3000 рублей, а в мае 2020 MasterCard до 5000. При этом решение о том, увеличивать лимит или нет, остается за банками. Предполагается, что злоумышленник, использующий POS-терминал для оплаты, может совершить незаконное списание денежных средств с банковского счета без ведома владельца, например, в общественном транспорте прислонить терминал с запросом на списание к сумке или карману.

Такой вариант развития событий, безусловно, возможен, однако на практике сложно реализуем в силу следующих обстоятельств:

1. Для осуществления данной операции необходимо небольшое расстояние между платежным терминалом и картой – менее 10 см [3]. Задача значительно усложняется, если в одном месте расположены несколько карт с возможностью бесконтактной оплаты, в случае обнаружения нескольких карт в поле действия некоторые виды терминалов не способны произвести списание денежных средств.
2. Важно понимать, что терминал нельзя так просто взять – он должен быть зарегистрирован, подключен, иметь доступ в Интернет, на него должен быть открыт счет, а организация, на которую открыт счет, должна пройти проверку службы безопасности банка. Злоумышленник может пользоваться POS-терминалом юридического лица, оформленного на подставные лица, однако стоимость таких компаний с расчетным счетом, подключенным эквайрингом и терминалом на черном рынке значительно превысит потенциальные выгоды от данного вида мошенничества, что делает его нецелесообразным.
3. Даже в случае успешного списания денежных средств у законных владельцев, их зачисление на счет злоумышленника произойдет не сразу, а по прошествии нескольких дней. При этом вероятность того, что никто из жертв не заметит пропажи и не обратится в свой банк-эмитент карты, а тот, в свою

очередь, в банк-эквайер с целью установления подозрительных операций по счету, который будет после заблокирован, крайне низка.

Следующий тип атаки – перехват данных, передающихся при обмене между терминалом и картой/смартфоном при оплате. Для ее осуществления необходимо специальное программно-аппаратное средство – сниффер. Перехват осуществляется, например, путем размещения антенны сниффера между терминалом и картой, что затруднительно сделать незаметно. При использовании данного способа могут быть перехвачены некоторые конфиденциальные данные, такие как номер карты, срок ее действия, имя владельца. Этих данных достаточно для совершения некоторых операций CNP – типа транзакций по банковским платежным картам, при которых держатель карты со своей картой физически не присутствует в момент и в месте проведения оплаты, например, при оплате в Интернет-магазине [4], [5].

Разберем разницу между видами бесконтактной оплаты. Существует несколько систем бесконтактной оплаты с мобильных устройств, к самым распространенным относятся Google Pay, Apple Pay и Samsung Pay. Все они работают по схожим принципам, но также между ними существует ряд некоторых отличий. Все три системы поддерживают NFC – ближнюю бесконтактную связь, используя которую они, как и бесконтактные пластиковые карты, обмениваются данными с платежными терминалами, которые также имеют ее поддержку. В то же время Samsung Pay реализует собственную технологию MST – имитацию магнитного сигнала, которая, имитируя магнитную полосу пластиковой карты, позволяет производить оплату почти на всех терминалах, в том числе и без поддержки NFC, что расширяет возможности пользователей данной системы.

В основе представленных систем лежит общая идея – токенизация платежей, которая позволяет сделать транзакции более безопасными. Технология токенизации позволяет заменить реальный номер карты клиента

уникальным сгенерированным кодом – токеном, который будет использован только для конкретной покупки, схема приведена на рис. 1.

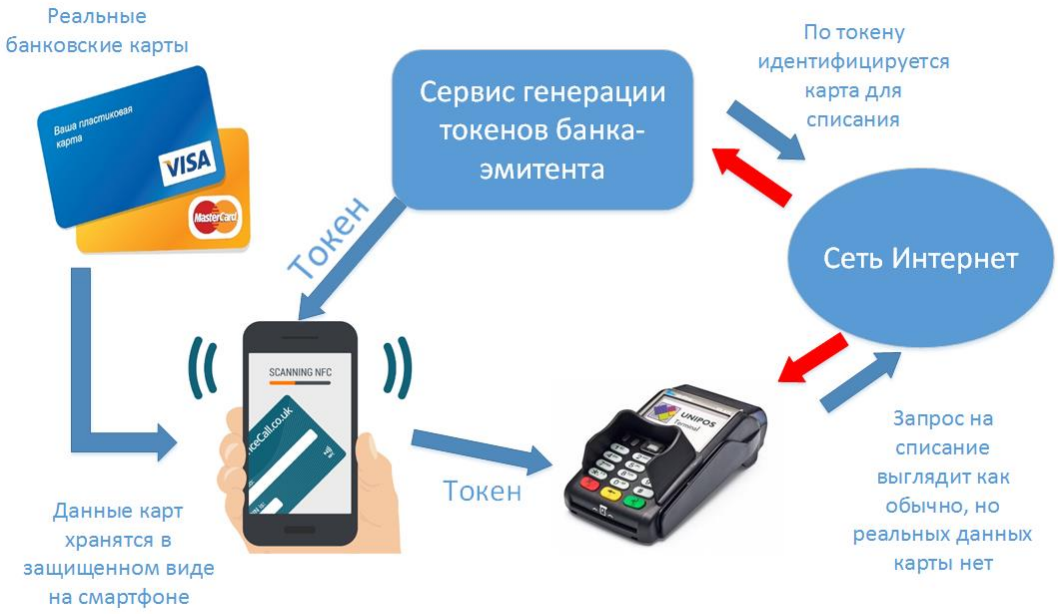

Рисунок 1. Схема совершения покупки. Рисунок автора.

Применение описанной технологии позволяет избежать одной из тех проблем, возникающих при оплате бесконтактной картой – во время обмена данными не передаются реквизиты реальной карты, лишь их виртуальные аналоги, обладая которыми постороннее лицо не сможет провести оплату. К тому же смартфон или другое мобильное устройство, в отличие от карты, не позволяет произвести считывание до совершения авторизации, то есть просто поднести терминал к смартфону не удастся, он его просто не «увидит».

Добавим, что в декабре 2019 года Советом по стандартам безопасности индустрии платежных карт PCI SSC опубликован текст спецификации PCI Contactless Payments on COTS (CPoC), устанавливающей правила безопасного приема платежей при помощи мобильных устройств. Данный стандарт призван обеспечить надежную защиту транзакций и позволит производителям расширить список оборудования для бесконтактного получения оплаты.

Ранее индустрия не имела единых норм безопасности программных и аппаратных решений, используемых продавцами для приема платежей. Стандарты устанавливались на уровне государства или отдельных корпоративных разработок, что ограничивало выбор продуктов и не обеспечивало должной безопасности покупок.

В PCI SSC ожидают, что первые устройства, сертифицированные по CPoC, появятся на рынке в 2020 году. Список верифицированных решений будет опубликован на сайте Совета. Некоммерческая организация ведет глобальный мониторинг угроз безопасности, связанных с использованием банковских карт, консультирует производителей, а также разрабатывает и поддерживает ряд стандартов в этой сфере [7]. Из этого можно сделать вывод, что использование устройства с одним из вышеперечисленных сервисов безопаснее, чем пользование обычной картой, поддерживающей бесконтактные платежи. Для исключения вероятности несанкционированного чтения бесконтактных карт можно применить экранирование, обернув карты фольгой или использовать кошелек с RFID защитой.

Список использованной литературы

1. НАФИ. Аналитический центр. [Электронный ресурс]: Бесконтактные платежи: возврата к наличным не будет. URL: https://nafi.ru/analytics/beskontaktnye-platezhi-vozvrata-k-nalichnym-ne-budet-/ (дата обращения: 26.06.2020).

2. Голдовский И. М. Банковские микропроцессорные карты. М.: Альпина Паблишер, 2010. 694 с.

3. ГОСТ Р ИСО/МЭК 14443-1-2013. Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 1. Физические характеристики: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013 г. № 1631-ст: дата введения 2015-01-01. – URL:

http://docs.cntd.ru/document/1200108020 (дата обращения: 28.06.2020). –Текст: электронный.

4. Хабр. [Электронный ресурс]: Как украсть деньги с бесконтактной карты и Apple Pay. URL: https://habr.com/ru/post/422551/ (дата обращения: 26.06.2020).

5. Кориков А. В., Литвиненко С. А., Москвин В. В. Мошенничество с платежными картами. Кардинг // Безопасность информационного пространства: сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Курган: Курганский государственный университет, 2016. С. 147–151.

6. Данилина Е. Ю., Ситникова А. А., Полякова Е. Н., Человечкова А. В. Использование биометрической идентификации на мобильных телефонах с целью обеспечения информационной безопасности пользователя // Актуальные проблемы правового обеспечения национальной безопасности в России: сборник материалов всероссийской научно-практической конференции. Курган: Курганский государственный университет, 2019. С. 60–66.

7. Threatpost. [Электронный ресурс]: CPoC: новый стандарт безопасности бесконтактных платежей. URL: https://threatpost.ru/pci-ssc-publishes-cpoc-security-standard/34982/ (дата обращения: 29.06.2020).

Гейн Александр Георгиевич
д. п. наук, профессор
Уральский федеральный университет
профессор, e-mail: a.g.geyn@urfu.ru, г. Екатеринбург, Россия
Косолобов Дмитрий Александрович
к. ф.-м. н., доцент
Уральский федеральный университет
e-mail: dkosolobov@mail.ru, г. Екатеринбург, Россия
Егоров Павел Владимирович
СКБ Контур, руководитель отдела,
e-mail: pe@skbkontur.ru, г. Екатеринбург, Россия