Библиографический список:

1. Российская Федерация. Налоговый Кодекс Российской Федерации (Часть 2, гл. 25): офиц. текст.- М.: Проспект, 2007. – 373с.

2. Российская Федерация. Законы. О бухгалтерском учете: федеральный закон от 06.12.11. № 402-ФЗ // Российская газета. – 2011. – № 278.

3. Божченко, Ж.А. Практические основы бухгалтерского учета источников формирования имущества организации: учебное пособие / Ж.А. Божченко. – Белгород: Белгородский государственный аграрный университет имени В.Я. Горина. – 2014. – 140 с.

4. Голованева, Е.А. Бухгалтерская технология проведения и оформления инвентаризации: учебное пособие / Е.А. Голованева. – Белгород: Белгородский государственный аграрный университет имени В.Я. Горина. – 2014. – 78 с.

5. Решетняк, Л.А. Документация: необходимость составления и возможность совершенствования / Л.А. Решетняк // Тезисы докладов на конференции «Проблемы сельскохозяйственного производства на современном этапе и пути их решения». – Белгород: Белгородский государственный аграрный университет имени В.Я. Горина. – 2014. – 285 с.

THE ORDER OF WRITE-OFF BAD DEBTS ALLOWANCE FOR DOUBTFUL DEBTS FOR EXAMPLE, LTD «GARDENS IN THE WOODS»

Koretsky Y.S., Bozhchenko J.A.

Keywords: *accounts receivable, allowance for Somni-tive debts, provision for reserve.*

The paper considers the methods of creating provision for doubtful debts (statistical, expert, interval) on a particular object of study.

УДК 004.056.53

УЯЗВИМОСТИ ПЛАТЕЖНЫХ СИСТЕМ

Корнеева Д.А., студентка 4 курса экономического факультета
Научный руководитель – Голубев С.В.,
кандидат экономических наук, доцент
ФГБОУ ВО Ульяновская ГСХА

Ключевые слова: *коммуникации, чип, платежные карты, атака,*

шифрование.

В статье рассмотрены различные особенности и уязвимости платежных систем

Будь то касса супермаркета, заправочная станция или интернет-магазин – безналичная оплата давно стала обычной в повседневной жизни. В будущем покупки будут осуществляться еще быстрее, преимущественно бесконтактным способом – с помощью специальных карт или смартфонов. В этой сфере финансовые институты делают ставку прежде всего на технологию NFC (Near Field Communication – коммуникация ближнего поля), которая позволяет записывать всю необходимую информацию на небольшой RFID-чип. Но опасности кроются не только в новых технологиях. Применяя все более изощренные методы, мошенникам удается проводить махинации с банкоматами, взламывают терминалы в магазинах, внедряют вредоносные программы через QR-коды и крадут миллионы с кредитных карт в результате только одной атаки.

То, что информация на кредитных картах с NFC-чипом не зашифрована, известно уже давно. Еще в феврале этого года хакер Кристин Паже продемонстрировала на хакерской конференции ShmooCon (Вашингтон, США) считывание номера кредитной карты и даты истечения ее срока действия. А на сегодняшний день уже существуют приложения для смартфонов, позволяющие получить такую информацию.

В конце июня соответствующее приложение было размещено даже на Play Market. Спустя некоторое время информация была удалена, но ее успели скачать от 100 до 500 раз, и на данный момент этот инструмент без проблем можно найти в Интернете.

Некоторые важные сведения не записываются на NFC-чип, например трехзначный CVV – код проверки подлинности, указываемый на обратной стороне карты. Таким образом, если злоумышленник захочет совершить покупку в интернете с помощью украденных данных, то это он сможет сделать только в магазинах, которые не требуют код проверки. Для MasterCard и Visa это определенный риск, которому подвержены и обыкновенные карты. Ведь в тот момент, когда клиент отдает карту (например, в кафе), каждый может скопировать номера, включая CVV. Но этот недостаток безопасности можно компенсировать, если подключить услугу SMS-уведомлений о произведенных транзакциях.

Опасность радиообмена смогли продемонстрировать два ученых из университета Тель-Авива в Израиле. С помощью их метода можно

записать весь обмен данными – как заявляют исследователи, даже в том случае, если карта и считывающее устройство используют усложненные алгоритмы аутентификации и шифрования.

В NFC-картах Sparkasse открывается доступ к последним 15 платежам и последним трем поступлениям. Банк рассматривает это как полезную услугу и даже предлагает приложения для считывания данной информации. Ну а специалисты по информационной безопасности, напротив, опасаются скрытого наблюдения за клиентами.

Так называемая Relay-атака проводится посредством самодельного считывающего устройства (Leech) и фальшивой карты (Ghost). С их помощью между картой клиента и считывающим устройством продавца подключается своего рода ретранслятор. За счет этого может быть реализован следующий сценарий атаки: злоумышленник приближается на улице к жертве, активирует своим считывателем карту клиента и передает данные на удаленную фальшивую карту своего сообщника, который, таким образом, может совершить покупку за средства жертвы.

Наибольшие трудности в проведении Relay-атаки у исследователей вызывало расстояние между картой клиента и считывателем, которое, согласно нормам ISO, составляет несколько сантиметров. Такое препятствие ученые преодолели, усилив сигнал, и добились вместо 10 см дистанции в 50 см. Для чистоты передачи данных специальное ПО фильтрует фоновые помехи. Считывающее устройство (Leech) перенаправляет данные на фальшивую карту (Ghost), которая может быть удалена на расстояние до 50 м. Трюк заключается в том, что эта карта содержит не пассивный NFC-чип, как в карте клиента, а активный, на который может производиться запись. Такой метод показывает, каких опасностей стоит ждать в будущем, после распространения NFC-карт.

Веб-сервисы это излюбленное место хакеров, так как в случае удачного проникновения в базу данных они получают сразу многочисленность имен, электронных адресов, данных учетных записей и номеров кредитных карт. Большинство людей используют одни и те же данные для авторизации на разных онлайн-платформах. Так что злоумышленникам нужно только сопоставить собранную информацию с платежными системами типа PayPal или «Яндекс.Денег» для того, чтобы похитить средства.

Очень часто продавцы используют QR-коды для предоставления клиентам дополнительной информации или для того, чтобы направить на страницу интернет-магазина. Так как QR-коды не показывают ссылку, которая скрывается за изображением, таким образом можно внедрить вредоносную программу или направить на фишинговый сайт.

Простым способом является, например, включение в сообщение электронной почты QR-кода вместо ссылки или завлечение пользователя на сайты мнимыми скидками.

Компания PayPal тестирует платежную систему PayPal Here, которая позволит любому смартфону принимать кредитные карты к оплате. Для этого продавцу нужно подсоединить считывающее устройство к телефону через гнездо наушников и устанавливает соответствующее приложение. Идея заключается в том, что в будущем любой человек сможет таким образом принимать оплату кредитной картой.

Злоумышленнику достаточно запустить работающее в фоновом режиме вредоносное ПО или скопировать приложение с дизайном PayPal или Square. Но на данный продавец может невольно стать соучастником хакера, если непреднамеренно загрузит на устройство вредоносную программу. Устройства от PayPal и Square считывают при сканировании карты информацию с магнитной полосы и функционируют пока только в США.

Магнитная полоса очень ненадежна и считается даже устаревшей, но, вопреки этому, все кредитные и дебетовые карты выпускаются с этой полосой. Эту уязвимость используют скиммеры для махинаций с банкоматом. Для предотвращения таких махинаций банки модернизируют свое оборудование. В банкоматах очень часто используется механизм «джиттер» и приемное устройство специальной антискимминговой формы.

В режиме «джиттер» карта втягивается в приемник резкими движениями вперед-назад, что делает практически невозможным считывание с магнитной ленты сторонними устройствами, а специальная форма приемника усложняет размещение накладки скиммера в приемном устройстве. В частности, из-за этого мошенники сосредоточились на более доступных целях. Последним трендом является проникновение в системы супермаркетов для манипуляций с их платежными устройствами.

Библиографический список:

1. Болтунова, И.И. Электронные деньги и электронные денежные системы / И.И. Болтунова, С.В. Голубев // Материалы II Всероссийской студенческой научной конференции «В мире научных открытий». – Ульяновск: УГСХА. – 2013. – С. 112 – 115.

2. Голубева, С.А. Актуальность создания национальной платежной системы РФ / С.А. Голубева, С.В. Голубев // Материалы IV Международной научно-практической конференции молодых ученых «Молодежь и наука XXI века». – Ульяновск: УГСХА, 2014. – С. 44 – 47.

3. Голубева, С.А. Проблемы развития электронных денег в России / С.А. Голубева, Е.А. Голубева // Материалы IV Международной научно-практической конференции «Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения». – Том III. – Ульяновск: УГСХА, 2012. – С. 53 – 59.

4. Кочетков, Н.М. Цели и методы наблюдения за платежными системами / Н.М. Кочеткова // Деньги и кредит. – 2013. – №1. – С. 12 – 15.

5. Криворучко, С.В. Организационная структура наблюдения за платежными системами / С.В. Криворучко // Финансы и кредит. – 2014. – № 12. – С. 71 – 76.

6. Латышева, Н.В. Некоторые аспекты развития платежных технологий в России / Н.В. Латышева // Финансы и кредит. – 2014. – № 12. – С. 14 – 17.

7. Полищук, С.А. Эффективная и безопасная национальная платежная система / С.А. Полищук // Банковское дело. – 2013. – № 11. – С. 13 – 15.

VULNERABILITIES OF PAYMENT SERVICE PROVIDERS

Korneeva D.A., Golubev S.V.

Keywords: *communications, chip, payment cards, attack, enciphering*

In article various features and vulnerabilities of payment service providers are considered

УДК 336.6

МЕТОДИЧЕСКИЕ АСПЕКТЫ УЧЕТА ПОТЕРЬ МАТЕРИАЛЬНЫХ ЦЕННОСТЕЙ ПРИ ЗАГОТОВЛЕНИИ И ХРАНЕНИИ В ПИЩЕВОЙ ПРОМЫШЛЕННОСТИ

Короткова С.В., студентка 3 курса учетно-финансового факультета
Научный руководитель – Кулиш Н.В., кандидат экономических наук, доцент
ФГБОУ ВО Ставропольский ГАУ

Ключевые слова: *потери материальных ценностей, виды потерь, учет потерь*