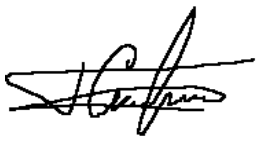
Системы дистанционного банковского обслуживания клиентов
через банкоматы и платёжные терминалы
(системы Д Б О)

Программное обеспечение MobilPay

Обеспечение безопасности в ПО MobilPay

Разработано: **ВНИПИ Спорт & MobilPay**

Генеральный директор
Г.А. Скрипников



Москва, 2016 год

С О Д Е Р Ж А Н И Е

Стр.

Данный документ является базовым документом, регламентирующим все вопросы обеспечения безопасности в системе ДБО с ПО MobilPay (ПО МР), начиная от разработки и внесения изменений в ПО МР и кончая эксплуатаций ПО МР в банках. Документ разработан с учётом требований аудитора PA DSS компании Digital Security и требований ряда банков РФ.

1. Введение

Настоящий документ содержит закрытую (для служебного внутрикорпоративного пользования) информацию об обеспечении безопасности программного обеспечения MobilPay (далее ПО МР). Под обеспечением безопасности понимается следующее:

- Обеспечение безопасности разработки и сохранности ПО МР
- Обеспечение безопасности распространения ПО МР на рынке
- Обеспечение безопасности и аудита действий персонала, эксплуатирующего ПО МР
- Обеспечение безопасности ПО МР при оказании финансовых услуг клиентам
- Обеспечение безопасности ПО МР при интеграции с другими системами банка
- Обеспечение требований стандарта безопасности PCI DSS и PA DSS
- Обеспечение безопасной работы с чиповыми картами EMV
- Обеспечение требований безопасности, предъявляемых банками

Документ предназначен для понимания общей концепции обеспечения безопасности ПО МР и принципов реализации отдельных компонент ПО МР, поддерживающих эту безопасность. Документ даёт также общее представление об обеспечении безопасности работы комплексной системы Дистанционного Банковского Обслуживания (далее ДБО) клиентов: «банкоматы/терминалы – процессинг – сервер MobilPay – АБС банка – биллинговые системы провайдеров услуг и посредников оплаты услуг».

Некоторые технические детали описания этих решений вынесены в отдельные Приложения, доступ персонала к которым вообще нежелателен (хранение в сейфе для исключительных случаев диагностики особых ситуаций при сопровождении ПО МР).

Благодаря наличию у банкоматов и платёжных терминалов специфических устройств (приёма наличных денег – депозитора, выдачи наличных денег – диспенсера, чтения банковских карт – картридера) и подключения банкоматов и терминалов к компьютерным системам банка и осуществляется дистанционное банковское самообслуживание клиента:

- Выдача наличных денег с карточных счетов клиента (СКС)
- Пополнение карточных счетов и счетов клиента в АБС банка
- Переводы средств со счёта на счёт
- Наличные и безналичные (по карте) платежи клиента различным провайдерам услуг и посредникам оплаты услуг – в режиме on-line или off-line
- Обмен валюты (покупка и продажа валюты за рубли)
- Погашение кредитов (с предоставлением клиенту информации о ходе погашения кредита)
- Денежные переводы через системы Юнистрим, Contact+, Western Union и др.
- Предоставление клиенту различной информации банка (баланса счёта, выписки по счетам, персональных предложений и рекламно-маркетинговой информации банка и др.)
- Предоставление клиенту услуг Интернет-банкинга (с виртуальной клавиатурой и печатью на чековом принтере)
- Предоставление клиенту услуг НПФ и страховых компаний
- Предоставление клиенту неплатёжных услуг (например, гос. услуг, услуг социальных карт и т.п.)
- Подключение и отключение различных сервисов банка, смена ПИН-кода и т.п.

При выполнении этих функций (услуг банковского самообслуживания клиента) ПО МР инициирует соответствующие запросы к процессингу и серверу MobilPay и обрабатывает ответные команды от них. Взаимодействие с этими серверами осуществляется по каналам связи. Само наличие финансовых операций уже требует обеспечения высокого уровня безопасности их выполнения (в частности, полную диагностику прохождения транзакций в системе, исключающую неконтролируемые причины возникновения финансовых убытков банка и клиентов). Кроме того, интеграция ПО МР с другими системами банка (с процессингом, АБС, биллингом) требует также чёткого разграничения ответственности ПО МР и других систем за результат работы комплексной системы в штатных и

нештатных ситуациях, с возможностью точной диагностики этой ответственности и обеспечения общей безопасности в системе, обеспечения сверки проведенных операций в АБС банка и внешних системах.

Кроме того, ПО МР и система банковского самообслуживания клиентов в целом постоянно развиваются. Приобретаются новые виды оборудования, расширяется набор услуг самообслуживания, подключаются новые провайдеры услуг и т.д. Поэтому идёт постоянный процесс обновления ПО МР новыми версиями. Это также требует определённой технологической дисциплины и мер безопасности.

Меняется также персонал, эксплуатирующий систему. Нельзя исключать случайные ошибки персонала, а также попытки несанкционированных действий персонала и посторонних лиц. Это также требует обеспечения полного контроля действий персонала (аудита), защиты от взлома системы и несанкционированных действий, мониторинга всех событий и ситуаций в системе, оперативного вмешательства и управления работой системы.

Имеются также внешние (установленные банками и платёжными системами VISA, MasterCard) стандарты и требования безопасности (PCI DSS, EMV, процессинговые протоколы DDC и NDC, ISO-8583 и т.п.), которые должны безусловно соблюдаться ПО МР.

2. Обеспечение безопасности разработки и сохранности ПО МР

2.1. Безопасность разработки программного обеспечения MobilPay

Для хранения эталонов ПО МР используется специальное хранилище (отв. главный конструктор ПО MobilPay) на двух компьютерах, установленных в разных местах на случай форс-мажорных обстоятельств.

Программисты работают только с копией модулей ПО МР. После тестирования осуществляется приёмка модуля главным конструктором ПО МР, осуществляющим сборку и генерацию программ для сервера, рабочих станций, банкоматов и терминалов в конфигурациях различных покупателей ПО МР. В результате получается конкретная версия (релиз) ПО МР, который тестируется на лабораторном стенде или тестовом стенде банка, а затем в опытной эксплуатации в системе банка.

Для координации и контроля разработки ПО МР используются следующие технологические системы:

- REDMINE (менеджмент и контроль заданий). Пример управления разработкой ПО МР приведен в Приложении R1.
- MERCURIAL (контроль изменений версий ПО МР, организация хранилища эталонов ПО МР и распределённых Back-up версий разрабатываемых или модифицируемых компонент ПО МР).

В работе используются все элементы промышленной технологии разработки ПО (псевдокоды, объектно-ориентированное и модульно-процедурное программирование, реляционная база данных, интерфейсы, несколько ступеней тестирования, соблюдение стандартов ISO-9000 и т.д.).

Все изменения ПО МР обязательно протоколируются и контролируются средствами системы MERCURIAL.

Со всеми программистами должны быть подписаны соглашения о соблюдении лицензионных прав, конфиденциальной информации и программных кодов компаний ВНИПИ Спорт и MobilPay, а также соблюдения технологической дисциплины разработки ПО МР (соглашения NDA).

Каждая новая версия ПО МР проходит несколько ступеней тестирования. В общем случае они включают в себя:

Э т а п		С о д е р ж а н и е т е с т а	**Исполнитель**
I	Unit Test	Отладка и рабочее тестирование ПО МР	Разработчик
II	Function Test	Функциональное тестирование ПО МР	Разработчик
III	Integration Test	Комплексное тестирование системы	Совместно

IV	Performance Test	Тесты производительности и критической нагрузки системы	Совместно
V	Reliability Test	Тесты надёжности	Совместно
VI	End-to-End Test	Контрольный тест полной готовности системы и персонала	Совместно
VII	Life Test	Опытная эксплуатация системы	Заказчик

В целом, эти этапы обеспечивают собственно разработку, отладку и настройку ПО МР разработчиком и совместное с заказчиком тестирование комплексной системы банка, завершая процесс испытаниями ПО МР в опытной эксплуатации, в реальных условиях.

Функциональный тест содержит помимо тестов корректного выполнения функций также тестирование ПО в условиях возникновения нештатных ситуаций. Создание нештатных ситуаций при выполнении конкретных функций является весьма сложной, творческой задачей. Часть нештатных ситуаций может возникать при нештатной работе других компонент системы, поэтому на этапе функционального теста могут быть оттестированы не все нештатные ситуации. Другая часть будет тестироваться при проведении интеграционного теста. Кроме того, некоторые нештатные ситуации вообще не могут быть искусственно вызваны, поэтому они могут быть выявлены и оттестированы только в процессе опытной (и даже промышленной) эксплуатации, а также специальными процедурами внешнего аудита (например, PCI DSS и EMV).

Интеграционный тест включает в себя прежде всего проверку совместной работы всех компонент ПО (MobilPay и других систем), проверку корректности взаимодействия систем (интерфейсов), корректное отражение результатов в базах данных всех систем, а также корректное реагирование на сбойные ситуации в различных системах и их компонентах.

Тест производительности и нагрузки предусматривает искусственное создание большого потока обрабатываемых данных (например, с помощью различных программ-эмуляторов на базе «захваченных» реальных потоков данных) с наблюдением реакции системы на критические нагрузки. Иногда здесь используются специальные средства тестирования. Иногда ограничиваются наблюдением реакции системы в реальных условиях (без проведения данного теста), предпринимая необходимые действия по усовершенствованию системы по мере возникновения проблем (достижения критических параметров нагрузки). Безусловно, реальный опыт эксплуатации является самым доверительным тестом производительности и нагрузочной способности системы, а средства повышения нагрузочной способности системы зависят, как правило, от конструкции системы и способности её к масштабированию.

Тест надёжности является весьма важным тестом, являясь одновременно инструментом обучения персонала, ответственного за действия в аварийных ситуациях. Он включает в себя испытания системы при искусственно создаваемых аварийных отключениях тех или иных компонент системы и проверку достаточности предусмотренных процедур нейтрализации и восстановления работоспособности системы после таких отключений (искусственных сбоев). Наиболее проблематичным здесь является искусственное создание аварийных ситуаций и выбор подходящего времени проведения таких испытаний до того, как аварийная ситуация может возникнуть в реальных условиях.

2.2. Защита базы данных MobilPay.

База данных MobilPay реализована на базе известной СУБД DB2 фирмы IBM, обеспечивающей свои мощные средства защиты безопасности данных (авторизацию пользователей и ограничение доступа). Кроме того, как уже отмечалось выше, для работы с базой данных DB2 требуется лицензия фирмы IBM.

Сами данные хранятся в СУБД DB2 в столь технически сложном формате, что работа с этими данными вне СУБД DB2 (с физически скопированными файлами) практически невозможна.

Кроме того, жесткие диски с данными, где хранится база данных MobilPay (БД МР) шифруются либо с помощью специальной настройки в Windows, либо с помощью задаваемых программ шифрования. Доступ к диску имеет только администратор сервера, который при запуске ОС должен ввести необходимые пароли. Ключи для шифрования меняются с регулярностью, указываемой правилами PCI DSS. Таким образом, полностью соблюдается правило PCI DSS о шифрации данных с

регулярной сменой ключей шифрования, с использованием одного из контуров аутентификации пользователей системы.

По существу, это является дополнительной информационной защитой при несанкционированном копировании дисков сервера MobilPay.

Необходимо отметить также, что и сам поток данных, поступающих на сервер MobilPay и исходящий от сервера MobilPay, также осуществляется в технически сложном формате протокола MP-2.3, расшифровать который при несанкционированном «перехвате» данных технически очень сложно. Вместе с общесистемной защитой сетевого доступа и общесистемной защитой базы данных DB2 это также является дополнительным защитным ресурсом информационной безопасности системы MobilPay.

Помимо указанных выше общесистемных средств некоторые конкретные данные в БД МР сами по себе хранятся в зашифрованном виде, для чего используются:

- Шифрация паролей операторов MobilPay – OPERATOR_PAROL_CRYPT.
- Шифрация в БД МР банковских карт – PAN_CRYPT (см. секретные приложения С1 и С2).

Иногда банки используют также технологию полной шифрации серверных дисков своих систем (или только дисков базы данных). В этом случае ПО МР вписывается в требуемую технологию банка.

2.3. Документирование проектных решений и изменений ПО МР.

Документация ПО МР включает в себя пользовательскую (эксплуатационную) и техническую (проектную) документацию, выпускаемую как на отдельные компоненты ПО МР, так и на систему в целом. Часть документации выпускается с грифом «ДСП» (для внутреннего служебного пользования).

3. Обеспечение безопасности распространения ПО МР на рынке

При поставках ПО МР покупателям (банкам) разработчик ПО МР с одной стороны обеспечивает защиту продаваемого ПО МР от несанкционированного использования, а с другой стороны – защиту репутации ПО МР, в том числе репутации безопасного программного обеспечения для банка и для клиентов банка.

Защита от несанкционированного использования ПО МР обеспечивается с помощью программно-аппаратных средств и технологии HASP фирмы Aladdin Software Security R.D., сертифицированных ФАПСИ в Российской Федерации.

При установке ПО МР на оборудовании банка обеспечивается безопасность процедуры установки сервера и рабочих станций MobilPay непосредственно специалистами поставщика ПО МР, либо под их контролем.

Массовая инсталляция ПО МР на банкоматах и терминалах осуществляется с использованием фиксированных образов диска, ограничивающих возможности вмешательства персонала в ПО МР и его настройки. При дальнейшей эксплуатации установленного ПО МР на банкоматах и терминалах осуществляется централизованный контроль и замена версий ПО МР и его настроек с рабочей станции оператора (администратора) системы MobilPay (с помощью компоненты ПО MP-Guard).

ПО МР на банкоматах и терминалах удовлетворяет всем требованиям безопасности PCI DSS. На банкоматах и терминалах устанавливается также антивирусное ПО и средства безопасности сетевого доступа.

Поставщик ПО МР обеспечивает гарантийное и после гарантийное сопровождение, оказывая помощь в диагностике нештатных ситуаций и гарантируя адекватную работу ПО МР в комплексной системе самообслуживания клиентов банка.

4. Ограничение доступа к функциям и данным ПО МР

В ПО МР реализована мощная и гибкая авторизация доступа операторов системы к функциям и данным MobilPay.

Для каждого сотрудника банка, работающего с системой (далее – оператора), обеспечивается авторизация, т.е. заведение его персональных данных и ограничение его доступа только к необходимым ему функциям. Оператор имеет собственный пароль (минимум 8 символов), хранящийся в базе данных MobilPay в зашифрованном виде. Шифрование осуществляется по секретному методу OPERATOR_PAROL_CRYPT.

Оператор в любое время может сменить пароль и должен это делать регулярно в соответствии с требованиями банка. Система MobilPay обеспечивает необходимые требования к качеству пароля и его сменяемости, хранение предыдущих паролей (для разборки ситуаций), заставляет пользователя менять пароли с заданным интервалом времени и т.п.

Система MobilPay всегда хранит и работает только с зашифрованными образами паролей. Это значит, что взятые из базы данных образы паролей невозможно использовать, не дешифрируя их. А введённый оператором (перед началом или в процессе работы) пароль всегда заново шифруется и сравнивается с хранящимся образом в базе данных. При совпадении результатов оператор может продолжить работу с системой MobilPay, в противном случае ему будет отказано.

Для каждого авторизованного оператора MobilPay отображает доступными только те функции (и, соответственно, данные), которые ему разрешены. Остальные функции видны как не доступные (disable). Такой принцип является общепринятым в программных пользовательских интерфейсах (GUI).

Для некоторых (особых) компонент ПО MobilPay, в частности для компоненты удалённого (централизованного) контроля и замены версий программного обеспечения и настроечных файлов на банкоматах, терминалах и рабочих станциях системы, чтения журналов и т.п., устанавливается дополнительный пароль доступа MP-Guard (дополнительное техническое ограничение работы инженерного персонала по эксплуатации ПО MobilPay).

В некоторых функциях (в частности, по требованию Сбербанка – при установке курсов обмена валют) применяется «парный» пароль (оператора и ответственного сотрудника банка). Выполнение этих функций возможно только при правильном вводе двух паролей двумя ответственными сотрудниками банка.

Доступ к базе данных MobilPay также ограничивается и средствами авторизации доступа к СУБД DB2 в дополнении к общей авторизации оператора ПО MobilPay.

Авторизацию операторов MobilPay выполняет Администратор эксплуатации MobilPay.

5. Операционный аудит действий персонала ПО МР

Каждое действие оператора в системе фиксируется в базе данных MobilPay, позволяя контролировать действия операторов в случае необходимости.

Журнализация всех действий персонала при работе с системой (изменение параметров системы, курсов валют, комиссии и т.д.) позволяет определять ответственность персонала при возникновении каких-либо ситуаций (операционный аудит). Эта функция системы прошла, в частности, весьма жёсткую сертификацию в Сбербанке РФ.

Безусловно, такому контролю подвержены только действия персонала, выполняемые средствами MobilPay. Если оператор имеет доступ к другим компьютерным ресурсам, он может выполнить их вне системы MobilPay. В этом случае ответственность за безопасность системы несёт администратор общесистемного (в т.ч. сетевого) доступа персонала ко всем компьютерным ресурсам. В то же время, MobilPay обеспечивает информационную защиту работы с данными при несанкционированном копировании, в частности – требования PCI DSS по защите данных о банковских картах и владельцах карт, PIN-кода и других кодов карты. В СУБД DB2 также предусмотрен собственный аудит DB2 с нужным объемом журнализации, который позволяет контролировать внешние действия администраторов системы при работе с СУБД (БД МР).

Помимо протоколирования действий персонала некоторые действия персонала отображаются оперативно в мониторинге MobilPay (открытие и закрытие дверей сейфа в банкоматах, выключение ПО МР и услуг на банкоматах и терминалах и др.). В этом случае дежурный оператор может немедленно выяснить причины таких действий и предпринять определённые действия для нейтрализации несанкционированных действий персонала или посторонних лиц.

6. Обеспечение безопасности ПО МР при оказании финансовых услуг клиентам

Прежде всего, безопасность обслуживания клиентов обеспечивается обязательно полной и корректной обработкой возникающих нештатных ситуаций при сбоях тех или иных технических средств на банкоматах и терминалах, и других компонент системы банковского самообслуживания

клиентов. В результате программное обеспечение содержит таких программных кодов больше, чем само выполнение операции (услуги) на банкомате и терминале.

ПО МР обеспечивает необходимые реакции на сбои устройств, реализует автоматические попытки восстановления работоспособности устройств банкомата и терминала командами Reset и т.п.

Некоторые действия ПО МР при возникновении нештатных (сбойных) ситуаций по требованию банков могут быть специфически (опционально) настраиваемы. Например, втягивание или не втягивание не взятых клиентом карт и денег, отключение или не отключение услуг при окончании бумаги в чековом принтере и т.д. В таких случаях ответственность за принятые решения берёт на себя банк.

Безусловно, в ПО МР ведётся полная журнализация всех действий клиента, всех сбоев, событий и ситуаций, происходящих как на банкомате/терминале, так и в других компонентах системы, что позволяет гарантировать достаточно точную и полную диагностику результата выполнения операции при возникновении претензий клиента или нестыковок в счётчиках инкассации банкоматов и терминалов.

Вся информация записывается в базе данных MobilPay и позволяет обращаться к анализу прошлых событий и проблемных операций, получать аналитические и статистические отчёты о работе системы и её отдельных компонент, в том числе для оценки безопасности работы системы при обслуживании клиентов.

7. Обеспечение безопасности ПО МР при интеграции с другими системами банка

7.1. Безопасность сетевого доступа.

Это первый, исключительно важный уровень ограничения доступа персонала при работе с любыми компонентами банковской системы (не только MobilPay), называемый иногда двухфакторной аутентификацией пользователей (с помощью специального физического ключа и пароля, которыми владеет каждый оператор индивидуально). Он реализуется известными общесистемными средствами, такими как RADIUS и TACACS с ключами или VPN (SSL/TLS или IPSEC) с индивидуальными «сертификатами». Сбербанк, например, работает с MobilPay и другими компонентами через специальные устройства ФПСУ. Выбор варианта этих средств делается банком.

Эти общесистемные средства являются также обязательными по требованию PCI DSS (пункт 8.3).

7.2. Безопасность используемых интерфейсов.

ПО МР использует стандартный протокол обмена сообщениями банкомата/терминала с процессингами (DDC и NDC со всеми известными «диалектами» этих протоколов от производителей банкоматов и процессингов) и сервера MobilPay с серверами процессингов различных производителей (POS, ISO-8583, Hosting Gate Way, Financial Transactions). Эти протоколы, в частности, обеспечивают необходимую шифрацию PIN-блока и макирование передаваемых сообщений ключами процессинга. Данная технология работы с процессингом полностью обеспечивается ПО МР и прошла сертификацию в компании OpenWay.

Для обмена данными сервера MobilPay с банкоматами, терминалами и рабочими станциями используется специально разработанный протокол МР-2.3. Разработка такого протокола была продиктована необходимостью снять ограничения протоколов DDC и NDC, а также обеспечить гарантированную доставку всех важных сообщений. Этот нечитабельный бинарный протокол также обеспечивает определённую защиту передаваемых данных от несанкционированного использования.

При обмене данными сервера MobilPay с шинами и серверами других систем банка и внешних систем используются применяемые ими способы шифрации (SSL и др.) для обеспечения безопасного обмена данными.

7.3. Обработка нештатных ситуаций.

При взаимодействии ПО МР с другими системами банка обеспечивается обработка различных нештатных ситуаций:

- Временное отключение канала связи (обработка превышения установленных таймаутов ожидания ответов на запросы)

- Ошибка в формате сообщения (например, при изменении интерфейсов в новых версиях биллинговых систем провайдеров услуг)
- Неожидаемый отказ в выполнении операции (после предварительной проверки возможности выполнения услуги в биллинговой системе провайдера)
- Неадекватная работа устройства при его некорректной настройке (например, кассет диспенсера)

И т.д.

В любом случае не допускается неопределённость реакции ПО МР (или тем более зависание ПО МР) при возникновении нештатных ситуаций в общей комплексной системе банка. Мониторинг ПО МР обеспечивает полную и точную диагностику всех нештатных ситуаций с точностью до кодов технических сбоев устройств по данным XFS производителей банкоматов и терминалов.

8. Обеспечение требований стандарта безопасности PCI DSS и PA DSS

Обеспечение требований безопасности PCI DSS при работе с MobilPay включает в себя:

- Ограничение сетевого доступа к MobilPay (общесистемными средствами)
- Хранение паролей доступа персонала к ПО МР в зашифрованном виде
- Не хранение данных о картах и владельцах карт, PIN-блока и других кодов карт на банкоматах и терминалах
- Хранение PAN карты на сервере MobilPay в зашифрованном виде
- Шифрование дисков с данными средствами Windows или другими программами шифрования

Первые две компоненты описаны выше. Ниже приведена информация о третьей и четвёртой компоненте обеспечения требований безопасности PCI DSS.

При считывании магнитной полосы или чипа банковской карты на банкомате или терминале эти данные используются только для формирования запроса к процессингу и не сохраняются. При записи в журнал или в базу данных MobilPay номер карты усекается (маскируется) в соответствии с требованиями PCI DSS, а PAN карты шифруется (см. секретное приложение С2).

При вводе клиентом PIN-кода он автоматически шифруется EPP клавиатурой, образуя шифрованный PIN-блок в соответствии с требованиями процессингов и международных платёжных систем VISA, MasterCard и др.

Этот зашифрованный PIN-блок и передаётся в процессинг в соответствии с общими требованиями безопасности PCI DSS и стандартами протоколов процессинга DDC и NDC.

На банкоматах и терминалах PIN-блок и другие карточные коды (CAV2, CID, CVC2, CVV2) не хранятся, на сервер и рабочие станции MobilPay эти данные не отправляются.

Таким образом, вся последующая работа операторов MobilPay с карточными данными при выполнении различных функций ПО МР и хранение результатов клиентских операций выполняется с маскированным номером карты и зашифрованными данными PAN банковских карт.

ПО МР прошло сертификацию на соблюдение стандартов PA DSS.

Информация о сертификации представлена на сайте PCI Security Standards Council:

https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php?agree=true&appname=MP-Terminal

Имея сертификацию PA DSS ПО МР неоднократно без проблем проходило сертификацию PCI DSS в различных банках в комплексе с другими системами банка.

Работа с полным номером карты в ПО МР используется только в компоненте «Персональные и автоматические платежи клиента», где операционист банка на своей рабочей станции в офисе банка заводит данные о клиенте банка и его персональных операциях (услугах банка). На этих же рабочих станциях операционист банка может также работать и с другими функциями АБС банка, связанными с карточными данными.

9. Обеспечение безопасной работы с чиповыми картами EMV

Безопасность работы ПО МР с чиповыми картами обеспечивается использованием сертифицированного EMV-ядра – программного модуля, поставляемого производителем банкомата или терминала, либо закупаемого банками, а также собственного программного модуля ПО МР-EMV.

ПО МР обеспечивает необходимую интеграцию ПО MobilPay-Terminal с сертифицированным EMV-ядром и гарантирует прохождение соответствующих EMV-тестов VISA и MasterCard.

10. Обеспечение требований безопасности, предъявляемых банками

В ряде случаев банки предъявляют собственные требования безопасности, которые реализуются в соответствии с договорными обязательствами поставщика ПО МР и банка.

Так, например, были реализованы специальные требования безопасности Сбербанка РФ, в соответствии с внутренними инструкциями банка: «Инструкции по настройке механизмов безопасности операционных систем семейства Windows персональных компьютеров сотрудников № 1252-р» и «Инструкции по настройке политики безопасности ОС Windows и BIOS SETUP» для терминалов, банкоматов и серверов.

В некоторых случаях ПО МР реализует несколько возможных схем выполнения операций, задание различных опций и параметров выполнения операций, которые самостоятельно задаются ответственными специалистами банка. В этом случае ответственность за принятые решения берёт на себя банк. Это же относится и к изменениям настроек процессинга специалистами банковского процессинга, могущих привести к финансовым и/или клиентским проблемам.

Во всех случаях компания-разработчик ПО МР проводит анализ специфических требований банка, предоставляя банку заключение о возможных нарушениях безопасности и повышенных рисках, отказываясь вносить опасные или рискованные технические решения в работу ПО МР и ДБО в целом.

Ниже приведено Приложение R1 «Пример Redmine-управления разработкой ПО МР», где по требованию аудитора PA DSS компании Digital Security представлен протокол аудит-контроля разработки и внесения изменений в ПО MobilPay в соответствии с требованиями безопасности PA DSS (4 примера).

Приложение R1. Пример Redmine-управления разработкой ПО МР.

Система Redmine позволяет руководителю проекта инициировать и контролировать работы различных специалистов по реализации разработки или модификации программного обеспечения MobilPay (далее ПО МР). Как правило, это задания на разработку, тестирование, проверку кода и документирование, выполняемы в рамках открытой руководителем «задачи» проекта.

Каждое задание специалисту автоматически направляется ему на адрес электронной почты (**см. примеры ниже**). Специалист, получив и выполнив задание, фиксирует его выполнение в системе Redmine, после чего руководитель проекта автоматически получает почтовое извещение Redmine и инициирует следующее назначение задания по данной задаче.

Система Redmine автоматически ведёт журнал всех назначений и выполнений заданий.

После выполнения всех необходимых заданий руководитель принимает решение о завершении всех работ и закрытии данной задачи.

В результате система Redmine обеспечивает полную историю выполнения всех заданий (см. заключительный экран в приведенных ниже примерах).

В системе хранятся все инициированные задачи с журналами истории реализации задачи вплоть до её полного выполнения и/или закрытия.

Ниже приводятся 4 примера управления разработкой (модификацией) ПО МР.

А) Примеры автоматических сообщений Redmine по электронной почте:

1-й ПРИМЕР – задача № 911:

1) По задаче #911 был создан начальный отчет-задание (Скрипников Георгий).

Новая функция #911: Реализовать новую опцию в ПО MP-Terminal: «Введение сдвоенных услуг, в частности услуги страхования детей»

- Автор: Скрипников Георгий
- Статус: Назначена
- Приоритет: Нормальный
- Назначена: Щепатов Андрей
- Категория:
- Версия:
- Функционал:

Суть задачи: при выполнении клиентом некоторых услуг предлагать ему дополнительные услуги.
Для этого необходимо добавить новую опцию Option_GoToInsurance в ПО MP-Terminal, чтобы определять «связку» двух услуг. В самой опции банк должен указывать номера "связанных" услуг.
Сами услуги добавляются специалистами банка самостоятельно. При образовании сдачи от наличной операции обеспечить предварительную обработку (использование) сдачи.

Подробнее техническое задание см. в документе "ТЗ по реализации опции GoToInsurance в MP-Terminal.doc"

это уведомление от Redmine. настройки уведомлений можно произвести, кликнув на ссылку "Моя учетная запись".

2) Задача #911 была обновлена (Щепатов Андрей).

- Параметр Дата выполнения изменился на 2013-11-06
- Параметр Статус изменился с Назначена на Решена
- Параметр Назначена изменился с Щепатов Андрей на Скрипников Георгий
- Параметр Готовность в % изменился с 0 на 100
- Параметр Оцененное время изменился на 6.00

Новая опция реализована в ПО МР-Т и оттестирована разработчиком.

Новая функция #911: Реализовать новую опцию в ПО MP-Terminal: «Введение сдвоенных услуг, в частности услуги страхования детей»

- Автор: Скрипников Георгий
- Статус: Решена
- Приоритет: Нормальный
- Назначена: Скрипников Георгий
- Категория:
- Версия:
- Функционал:

Суть задачи: при выполнении клиентом некоторых услуг предлагать ему дополнительные услуги.
Для этого необходимо добавить новую опцию Option_GoToInsurance в ПО MP-Terminal, чтобы определять «связку» двух услуг. В самой опции банк должен указывать номера "связанных" услуг.
Сами услуги добавляются специалистами банка самостоятельно. При образовании сдачи от наличной операции обеспечить предварительную обработку (использование) сдачи.

Подробнее техническое задание см. в документе "ТЗ по реализации опции GoToInsurance в MP-Terminal.doc"

это уведомление от Redmine. настройки уведомлений можно произвести, кликнув на ссылку "Моя учетная запись".

3) Задача #911 была обновлена (Скрипников Георгий).

- Параметр Статус изменился с Решена на Назначена
- Параметр Назначена изменился с Скрипников Георгий на Половинкин Кирилл

Провести независимое тестирование новой опции, а также функциональное тестирование ПО MP-T.

Новая функция #911: Реализовать новую опцию в ПО MP-Terminal: «Введение сдвоенных услуг, в частности услуги страхования детей»

- Автор: Скрипников Георгий
- Статус: Назначена
- Приоритет: Нормальный
- Назначена: Половинкин Кирилл
- Категория:
- Версия:
- Функционал:

Суть задачи: при выполнении клиентом некоторых услуг предлагать ему дополнительные услуги.
Для этого необходимо добавить новую опцию Option_GoToInsurance в ПО MP-Terminal, чтобы определять «связку» двух услуг. В самой опции банк должен указывать номера "связанных" услуг.
Сами услуги добавляются специалистами банка самостоятельно. При образовании сдачи от наличной операции обеспечить предварительную обработку (использование) сдачи.

Подробнее техническое задание см. в документе "ТЗ по реализации опции GoToInsurance в MP-Terminal.doc"

это уведомление от Redmine. настройки уведомлений можно произвести, кликнув на ссылку "Моя учетная запись".

4) … Независимое тестирование…

5) … Назначение проверки кода и уязвимостей…

6) … Проверка кода и уязвимостей…

7) … Назначение документирования…

8) Задача #911 была обновлена (Скрипников Анатолий).

В документ «Описание опций Scenario_ServOption» добавлено краткое описание возможности самостоятельного задания специалистами банка сдвоенных услуг с помощью новой опции Option_GoToInsurance в ПО MP-Scenario.

Новая функция #911: Реализовать новую опцию в ПО MP-Terminal: «Введение сдвоенных услуг, в частности услуги страхования детей»

- Автор: Скрипников Георгий
- Статус: Назначена
- Приоритет: Нормальный
- Назначена: Скрипников Георгий
- Категория:
- Версия:
- Функционал:

Суть задачи: при выполнении клиентом некоторых услуг предлагать ему дополнительные услуги.
Для этого необходимо добавить новую опцию Option_GoToInsurance в ПО MP-Terminal, чтобы определять «связку» двух услуг. В самой опции банк должен указывать номера "связанных" услуг.
Сами услуги добавляются специалистами банка самостоятельно. При образовании сдачи от наличной операции обеспечить предварительную обработку (использование) сдачи.

Подробнее техническое задание см. в документе "ТЗ по реализации опции GoToInsurance в MP-Terminal.doc"

это уведомление от Redmine. настройки уведомлений можно произвести, кликнув на ссылку "Моя учетная запись".

9) Задача #911 была обновлена (Скрипников Георгий).

- Параметр Статус изменился с Назначена на Закрыта

Информирую всех участников проекта о завершении модификации ПО MP – добавление возможности сдвоенных услуг клиента.
Новую версию ПО MP-Terminal включаем в релиз для Заказчиков. Задачу закрываем.

Всем спасибо!

Новая функция #911: Реализовать новую опцию в ПО MP-Terminal: «Введение сдвоенных услуг, в частности услуги страхования детей»

- Автор: Скрипников Георгий
- Статус: Закрыта
- Приоритет: Нормальный
- Назначена: Скрипников Георгий
- Категория:
- Версия:
- Функционал:

Суть задачи: при выполнении клиентом некоторых услуг предлагать ему дополнительные услуги.
Для этого необходимо добавить новую опцию Option_GoToInsurance в ПО MP-Terminal, чтобы определять «связку» двух услуг. В самой опции банк должен указывать номера "связанных" услуг.
Сами услуги добавляются специалистами банка самостоятельно. При образовании сдачи от наличной операции обеспечить предварительную обработку (использование) сдачи.

Подробнее техническое задание см. в документе "ТЗ по реализации опции GoToInsurance в MP-Terminal.doc"

это уведомление от Redmine. настройки уведомлений можно произвести, кликнув на ссылку "Моя учетная запись".

В результате:

Все задания руководителя проекта выполнены.

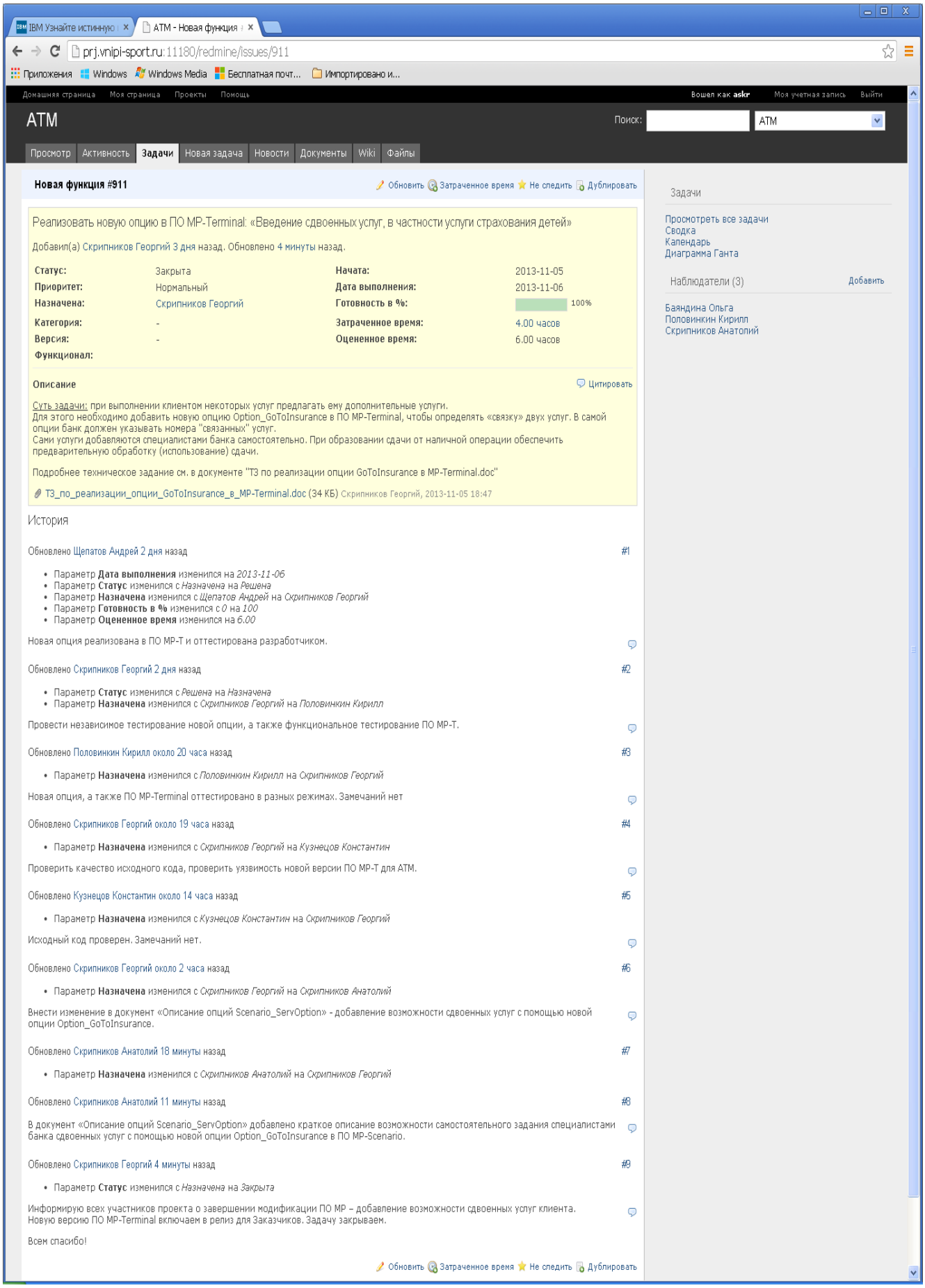
Модифицированная версия ПО MP прошла независимое тестирование, проверку кода и уязвимостей.

Изменения задокументированы.

Новая версия ПО MP принята руководителем проекта.

Задача закрыта.

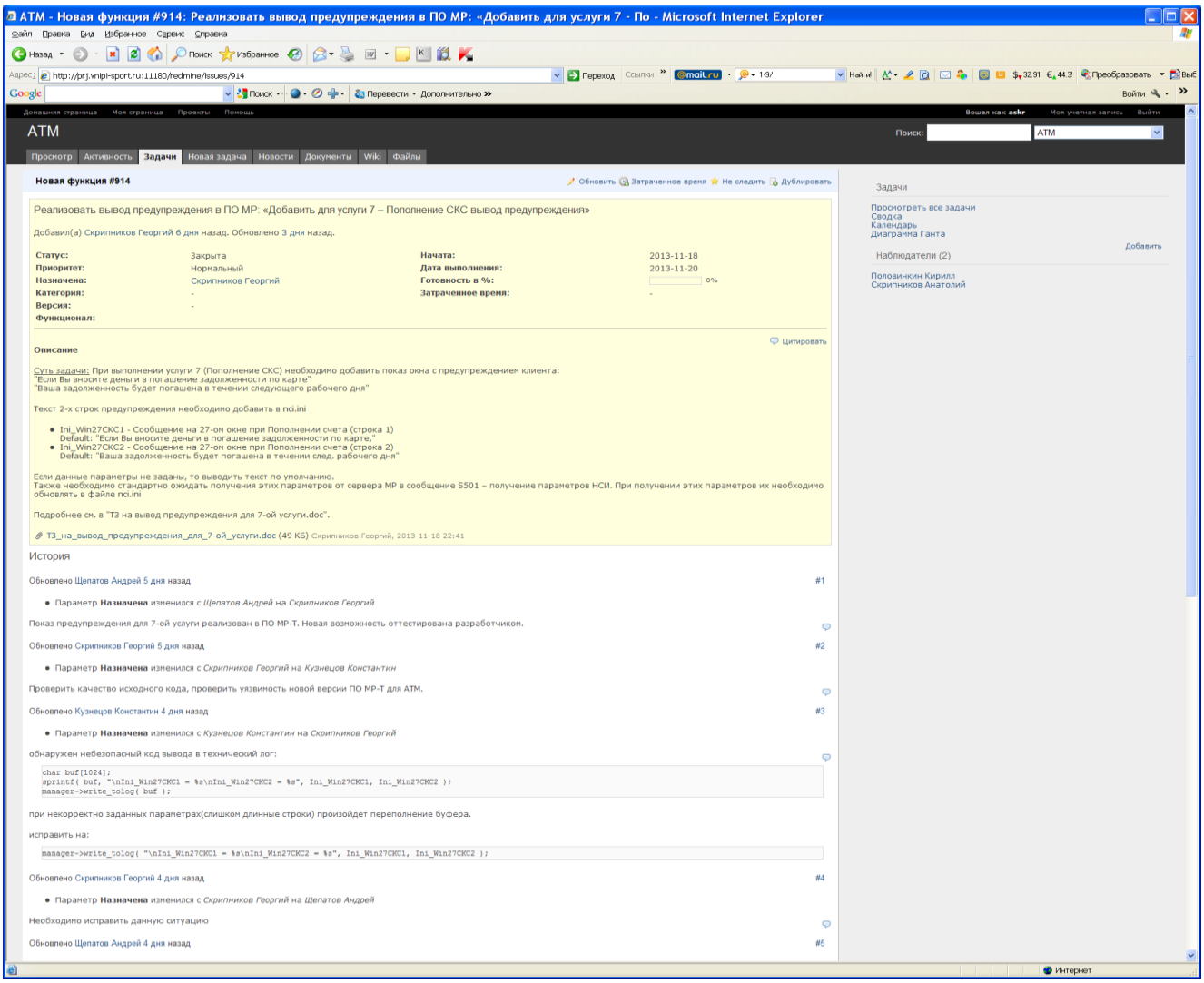
Б) Итоговый журнал Redmine с историей действий персонала по реализации задачи # 911.



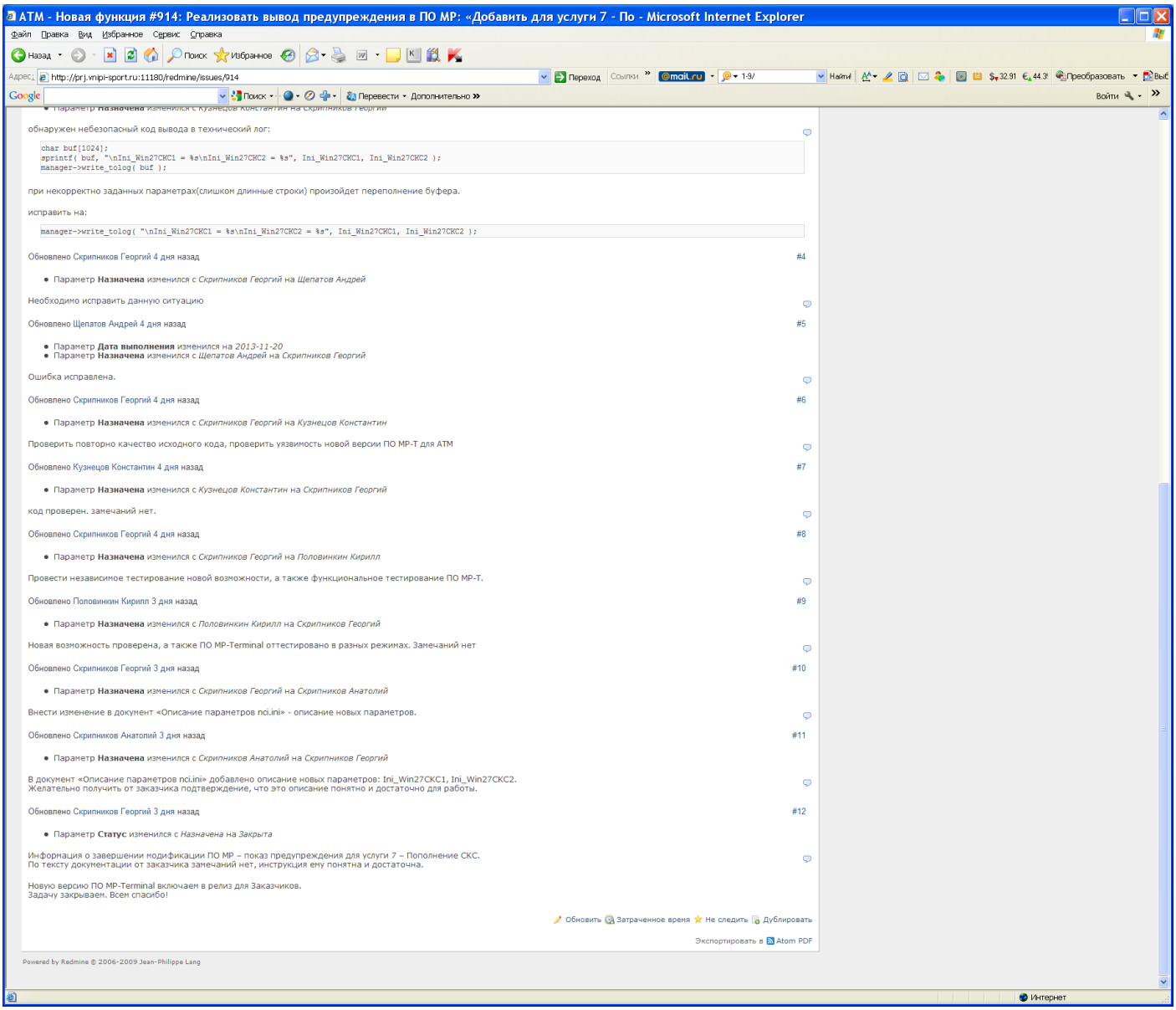
2-й ПРИМЕР – задача № 914: Реализовать вывод предупреждения в ПО МР «Добавить для услуги 7 – Пополнение СКС вывод предупреждения»

Повторная проверка кода ПО МР на уязвимость.

Итоговый журнал Redmine с историей действий персонала по реализации задачи # 914.



Продолжение экрана Redmine для задачи № 914:



3-й ПРИМЕР – задача № 1411: Реализация требования МТС вывода в чеке обязательной строки "Платёж выполнен без акцептования МТС".

Итоговый журнал Redmine с историей действий персонала по реализации задачи # 1411.

Редактировать | Трудозатраты | Следить

Новая функция #1411

Реализация требования МТС вывода в чеке обязательной строки "Платёж выполнен без акцептования МТС"

Добавил(а) Скрипников Георгий 6 дня назад. Обновлено около 10 часа назад.

Статус:	Закрыта	**Дата начала:**	2016-12-08
Приоритет:	Нормальный	**Дата завершения:**	
Назначена:	Скрипников Анатолий	**Готовность:**	0%
Функционал:			

Описание — Цитировать

Суть задания: Необходимо добавить в печатаемый чек для провайдера МТС (для наличной и безналичной услуги) строку "Платёж выполнен без акцептования МТС".

модификации ПО МР выполнить **Щепатову Андрею** в соответствии с постановкой задачи.

История

Обновлено Щепатов Андрей 2 дня назад #1

- Параметр **Статус** изменился с *Назначена* на *Решена*

Данная доработка выполнена в ПО MP-Terminal и оттестирована разработчиком.

Обновлено Скрипников Георгий 2 дня назад #2

- Параметр **Статус** изменился с *Решена* на *Назначена*
- Параметр **Назначена** изменился с *Щепатов Андрей* на *Васильев Алексей*
- Параметр **Приоритет** изменился с *Высокий* на *Нормальный*

Провести независимое тестирование доработки ПО MP-Terminal, а также функциональное тестирование ПО MP-Terminal на АТМ

Обновлено Васильев Алексей около 24 часа назад #3

- Параметр **Статус** изменился с *Назначена* на *Решена*

Данная доработка, а также функции ПО MP-Terminal оттестированы в разных режимах. Замечаний нет.

Обновлено Скрипников Георгий около 23 часа назад #4

- Параметр **Статус** изменился с *Решена* на *Назначена*
- Параметр **Назначена** изменился с *Васильев Алексей* на *Кузнецов Константин*

Проверить качество исходного кода, проверить уязвимость новой версии ПО MP-Terminal для АТМ

Обновлено Кузнецов Константин около 17 часа назад #5

- Параметр **Статус** изменился с *Назначена* на *Решена*

Исходный код проверен. Замечаний нет.

Обновлено Скрипников Георгий около 17 часа назад #6

- Параметр **Статус** изменился с *Решена* на *Назначена*
- Параметр **Назначена** изменился с *Кузнецов Константин* на *Скрипников Анатолий*

Расширить документацию с формами и примерами чеков.

Обновлено Скрипников Анатолий около 10 часа назад #7

В документацию добавлено уточнение печати чека для МТС.

Обновлено Скрипников Георгий около 10 часа назад #8

- Параметр **Статус** изменился с *Назначена* на *Закрыта*

Информирую всех участников проекта о завершении модификации ПО MP-Terminal – **добавление специальной строки при печати чека для услуги МТС («Платёж выполнен без акцептования МТС»).**
Новую версию ПО MP-Terminal включаем в релиз для Заказчиков.
Задачу закрываем. Всем спасибо!

Редактировать | Трудозатраты | Следить

Экспортировать в Atom | PDF

4-й ПРИМЕР – задача № 1409: Верификация телефонов через СМС подтверждение в маркетинговой компоненте ПО МР.

Итоговый журнал Redmine с историей действий персонала по реализации задачи # 1409.

Редактировать | Трудозатраты | Следить

Новая функция #1409

Верификация телефонов через СМС подтверждение в маркетинговой компоненте

Добавил(а) Скрипников Георгий 6 дня назад. Обновлено около 10 часа назад.

Статус:	Закрыта	**Дата начала:**	2016-12-08
Приоритет:	Нормальный	**Дата завершения:**	
Назначена:	Скрипников Анатолий	**Готовность:**	0%
		Трудозатраты:	7.50 ч
Функционал:			

Описание

Цитировать

Суть задания: Необходимо расширить маркетинговую компоненту ПО MobilPay (далее ПО МР), добавив в системе новый признак «Нужно ли верифицировать телефон через СМС или нет?».
При необходимости верификации необходимо предоставить клиенту экран для ввода номера телефона. После ввода телефона нужно послать СМС-уведомление через сервер МР. После получения от сервера подтверждения, что СМС отправлена перейти на экран с вводом одноразового пароля подтверждения операции. После успешного подтверждения клиентом пароля терминал должен послать сообщение на сервер МР для записи обновлённого номера телефона клиента в базу данных МР, после чего перейти к выполнению услуги на терминале.
Подробнее техническое задание см. в документе **"ТЗ по верификации телефона через СМС через маркетинг.doc"**

Реализовывать будет **Дёмин Александр**.
Выполнить необходимую доработку ПО МР в соответствии с постановкой задачи и ТЗ.

Верификация телефона через маркетинговую компоненту.rar (1,3 МБ) Скрипников Георгий, 2016-12-08 12:58

История

Обновлено Дёмин Александр 2 дня назад #1

- Параметр **Статус** изменился с *Назначена* на *Решена*

Данная доработка выполнена в ПО MP-Terminal и оттестирована разработчиком.

Обновлено Скрипников Георгий 2 дня назад #2

- Параметр **Статус** изменился с *Решена* на *Назначена*
- Параметр **Назначена** изменился с *Дёмин Александр* на *Половинкин Кирилл*

Провести независимое тестирование новой опции, а также функциональное тестирование ПО MP-Terminal

Обновлено Половинкин Кирилл около 21 часа назад #3

- Параметр **Статус** изменился с *Назначена* на *Решена*

Новый функционал, а также ПО MP-Terminal оттестированы в разных режимах. Замечаний нет.

Обновлено Скрипников Георгий около 21 часа назад #4

- Параметр **Статус** изменился с *Решена* на *Назначена*
- Параметр **Назначена** изменился с *Половинкин Кирилл* на *Кузнецов Константин*

Проверить качество исходного кода, проверить уязвимость новой версии ПО MP-Terminal для АТМ

Обновлено Кузнецов Константин около 17 часа назад #5

- Параметр **Статус** изменился с *Назначена* на *Решена*

Исходный код проверен. Замечаний нет.

Обновлено Скрипников Георгий около 17 часа назад #6

- Параметр **Статус** изменился с *Решена* на *Назначена*
- Параметр **Назначена** изменился с *Кузнецов Константин* на *Скрипников Анатолий*

Расширить документацию по показу персональных и маркетинговых предложений клиентам с учётом новых доработок.

Обновлено Скрипников Анатолий около 11 часа назад #7

В документацию внесены соответствующие изменения.

Обновлено Скрипников Георгий около 10 часа назад #8

- Параметр **Статус** изменился с *Назначена* на *Закрыта*

Информирую всех участников проекта о завершении модификации ПО MP-Terminal – **добавление возможности верификации телефонов в маркетинговую компоненту ПО МР.**
Новую версию ПО MP-Terminal включаем в релиз для Заказчиков.
Задачу закрываем. Всем спасибо!

Редактировать | Трудозатраты | Следить

Секретное Приложение С1.

Предоставляется только в исключительных случаях.

Секретное Приложение С2.

Предоставляется только в исключительных случаях.