uniPayment-сервис

Руководство по внедрению в соответствии с требованиями PCI DSS

Всего листов: 15

Версия: 1 rev. 1.04
Дата создания: 2011-11-23

Москва, 2011

Содержание:

Термины и определения

Термин	Определение
PA-DSS	Payment Application Data Security Standard Стандарт безопасности данных платёжных приложений, содержащий требования к разработке, внедрению и эксплуатации программных решений, участвующих в обработке платёжных транзакций, в соответствии с требованиями PCI DSS.
PCI DSS	Payment Card Industry Data Security Standard Стандарт защиты информации в индустрии платёжных карт, набор требований к безопасности данных о держателях карт, разработанный международными платёжными системами VISA, MasterCard, American Express, JCB, Discover.
PCI SSC	Payment Card Industry Security Standards Council Совет по стандартам безопасности индустрии платёжных карт
PIN	См. «ПИН»
Uniteller	См. «Компания»
Авторизация	Процесс предоставления прав доступа или других полномочий пользователю, программе или процессу.
Данные о держателях карт	PAN, имя держателя карты, срок действия карты, сервисный код
Держатель карты или Покупатель	Владелец банковской платёжной карты, использующий её для осуществления покупки.
Компания, Uniteller	АО «Предпроцессинговый расчетный центр»
Мёрчант	См. «Предприятие»
ПИН	Персональный идентификационный номер — секретная последовательность цифр, используемая для идентификации держателя карты.
Платёжный терминал, терминал	Совокупность оборудования и программного обеспечения Торговой точки, обеспечивающая возможность продажи товаров/услуг с оплатой за них банковской картой в режиме самообслуживания.
ПО	Программное обеспечение
Чувствительные данные	Полные данные магнитной полосы карты или её эквивалент на чипе, CAV2/CVC2/CVV2/CID, PIN/PIN-блок

Введение

Этот документ является Руководством по внедрению в соответствии с требованиями стандарта PCI DSS (PA-DSS Implementation Guide) при внедрении платёжного сервиса uniPayment.

Руководство предназначено представителям мерчантов и сервис-провайдеров платёжных решений, а также всем другим заинтересованным лицам, участвующим в интеграции uniPayment-сервиса в платёжные системы.

Руководство рассматривает функционал uniPayment-сервиса с точки зрения выполнения требований стандартов PCI DSS по работе с платёжными данными, а также содержит предписания по установке и настройке сервиса, обеспечивающие соответствие сервиса требованиям стандарта PCI DSS.

Информация о Payment Application Data Security Standard

Стандарт Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS или PA-DSS, стандарт безопасности данных платёжных приложений) разработан Советом по стандартам безопасности индустрии платёжных карт (Payment Card Industry Security Standards Council, PCI SSC) и содержит требования к разработке, внедрению и эксплуатации программных решений, участвующих в обработке платёжных транзакций, в соответствии с требованиями PCI DSS. Требования PA-DSS являются производными от требований и процедур оценки безопасности PCI DSS.

По решению международных платёжных систем Visa и MasterCard все торгово-сервисные предприятия (мерчанты) и поставщики услуг начиная с 1 июля 2012 года должны использовать только сертифицированные по стандарту PA-DSS платёжные приложения. Контроль выполнения этого требования возложен на банки-эквайеры. Сертификацию платёжных приложений по стандарту PA-DSS могут выполнять компании, обладающие статусом PCI PA-QSA.

Требования стандарта PA-DSS распространяются на продаваемые на рынке приложения, обеспечивающие процесс авторизации или оплаты в платёжных системах.

Стандарт применим только к тем модулям продукта, которые непосредственно выполняют платёжные функции.

1 Общая информация о uniPayment-сервисе

Платёжный uniPayment-сервис является универсальной программной компонентой, реализующей всю платёжную логику в одном приложении и интегрируемой с подавляющим большинством OLE оборудованием платёжных терминалов.

uniPayment-сервис устанавливается на программно-аппаратный комплекс (терминал) Предприятия и может работать под управлением следующих операционных систем:

- Windows 7;
- Windows 7 for Embedded Systems;
- Windows XP;
- Windows XP for Embedded Systems;
- Windows 2000;
- Работа под Wine версии 1.3 и выше в Linux на ядре 2.6 и выше (например, Red Hat, Fedora, CentOS 5.5).

Ключевые функциональные возможности uniPayment:

- Использование EFTPOS-протокола в качестве базового, что даёт возможность взаимодействия с приложением терминала по TCP/IP или в режиме эмуляции RS232.
- Поддержка OEM-оборудования (ПИН-клавиатуры, считыватели карт, принтеры чеков и др.) разных производителей, подключаемого по интерфейсам RS232 или USB.
- Возможность работы как с экраном, встроенным в ПИН-клавиатуру, так и с основным экраном терминала, управляемым ПО терминала.
- Поддержка стандарта EMV (Level 2).
- Возможность установления VPN-соединения с авторизационным хостом.

Поддерживаемые протоколы:

- VisaLight
- IFX, IFX2, IFX 3 (Uniteller)
- EFTPOS
- EPI
- KISS

2 Общие требования для обеспечения безопасного использования uniPayment-сервиса

Для обеспечения безопасного использования uniPayment-сервиса, в частности, при передаче данных по общедоступным и беспроводным сетям, следует обеспечить выполнение следующих требований:

– На каждом терминале должен быть настроен межсетевой экран в соответствии с заранее утверждённой конфигурацией. Для утверждения конфигурации необходимо создать актуальную схему сети, в которой будут указаны все каналы доступа к терминалу и каналы, по которым будет осуществляться передача данных от терминала к хосту процессинга, включая все беспроводные сети. В соответствии с этой схемой конфигурация межсетевого экрана должна запрещать все соединения между недоверенными сетями и всеми системными компонентами. Адрес и порт, используемый сервисом для обращения на хост процессинга, указывается в конфигурационном файле **EFTPOS_Uniteller.ini** в разделе [**Host**], параметры **Address** и **Port**, соответственно. Эти адрес и порт должны быть включены в конфигурацию как разрешённые для программы **СЕРВИС**. В случае если связь между ПО терминала и сервисом осуществляется по протоколу TCP, то порт, используемый для связи между ними, должен быть включён в конфигурацию только для этих программ.
Примечание: *недоверенной является любая сеть, внешняя по отношению к сетям клиента и/или сеть, которая им не контролируется.*

– В соответствии с требованиями п. 4 стандарта PCI DSS «Обеспечить шифрование данных о держателях карт при их передаче через сети общего пользования» для безопасной передачи данных до хоста эквайера клиент должен использовать стойкие криптографические алгоритмы и безопасные протоколы (например, такие как SSL/TLS, IPSEC, SSH и т. д.). Конфигурацию канала связи требуется дополнительно согласовать с процессинговым центром.
При осуществлении процессинга платежей через процессинговый центр Uniteller для организации защищённого канала связи необходимо использовать программу OpenVPN,

которую можно загрузить по адресу: http://openvpn.net/index.php/open-source/downloads.html. В этом случае используется IFX-протокол для запросов к хосту, а в качестве транспортного протокола — HTTPS. В остальных случаях для запросов к хосту используется протокол ISO8583, и в качестве транспортного протокола — TCP. В этом случае для шифрования трафика с хостом необходимо включить шифрование пакетов, присвоив параметру **enable_SecureISO** в секции [**Protocol**] конфигурационного файла сервиса (файл **EFTPOS_Uniteller.ini**) значение **true**.

3 Роли и обязанности сторон

3.1 Участники сообщества платёжных приложений

Жизненный цикл платёжного uniPayment-сервиса связан со следующими участниками сообщества платёжных приложений:

- Разработчик ПО uniPayment-сервиса и uniPayment-компоненты.
- Дилеры и системные интеграторы.
- Клиенты.

Каждый из участников для соответствия комплексного платёжного решения требованиям стандартов PA-DSS и PCI DSS должен обеспечить выполнение ряда требований, рассмотренных ниже.

3.2 Обязанности разработчика uniPayment-сервиса

Разработчиком uniPayment-сервиса, а также производителем uniPayment-компоненты является АО «Предпроцессинговый расчетный центр». С точки зрения подтверждения продукта требованиям стандарта PA-DSS разработчик имеет следующие обязанности:

- Разработка платёжного приложения (приложений), соответствующего стандарту PA-DSS, обеспечивающего соответствие сети клиента стандарту PCI DSS и не препятствующего этому.
- Разработка для каждого платёжного приложения Руководства по применению стандарта PA-DSS (PA-DSS Implementation Guide; этот документ).
- Обучение клиентов, дилеров и системных интеграторов тому, как следует устанавливать и настраивать платёжное приложение в соответствии с требованиями стандарта PCI DSS.

3.3 Обязанности дилера и системного интегратора

Дилеры и системные интеграторы — это организации, которые продают, устанавливают и/или обслуживают платёжные приложения от имени производителей ПО или других компаний. С точки зрения подтверждения продукта требованиям стандарта PA-DSS дилер и системный интегратор имеет следующие обязанности:

- Обеспечение интеграции платёжного приложения, соответствующего требованиям стандарта PA-DSS, в среду, соответствующую требованиям стандарта PCI DSS.
- Выбор конфигурации платёжного приложения должен выполняться в соответствии с Руководством по применению стандарта PA-DSS (этот документ).
- Выбор конфигурации среды, в которую интегрируется платёжное приложение, должно выполняться в соответствии с требованиями стандарта PCI DSS.
- Обслуживание платёжного приложения (например, устранение неполадок, получение обновлений из сети Интернет и предоставление удалённой технической поддержки) должно выполняться в соответствии с Руководством по применению стандарта PA-DSS (этот

документ).

3.4 Обязанности клиента

Клиенты — это торгово-сервисные предприятия, сервис-провайдеры или другие организации, которые приобретают или получают платёжное приложение третьей стороны для хранения, обработки или передачи данных платёжных карт при авторизации или сеттлементе платёжных транзакций. С точки зрения подтверждения продукта требованиям стандарта PA-DSS клиент имеет следующие обязанности:

- Платёжное приложение, соответствующее стандарту PA-DSS, должно реализовываться в среде, соответствующей требованиям стандарта PCI DSS.
- Выбор конфигурации платёжного приложения должен выполняться в соответствии с Руководством по применению стандарта PA-DSS (этот документ).
- Выбор конфигурации среды, в которую интегрируется платёжное приложение, должно выполняться в соответствии с требованиями стандарта PCI DSS.
- Должно обеспечиваться управление статусом конфигурации среды и платёжного приложения в соответствии с требованиями стандарта PCI DSS.

4 Соответствие uniPayment-сервиса требованиям стандарта PA-DSS

4.1 Удаление критичных данных авторизации, сохранённых предыдущими версиями приложения (требование 1.1.4)

- В текущей версии uniPayment-сервиса никаких критичных данных не хранится.
- Предыдущие версии могли записывать в логах критичные данные. Поэтому после обновления версии сервиса требуется очистить папку, содержащую логи.
- Журналы хранятся в папке, указанной в параметре **log_folder** в конфигурационном файле (по умолчанию, папка Logs).
- Для очистки ранее сохранённых критичных данных требуется удалить файлы журналов с использованием программы «гарантированного удаления» данных, например, следующие:
  - Eraser (официальный сайт по адресу: http://www.heidi.ie/).
  - BCWip (официальный сайт по адресу: http://www.jetico.com/data-protection-wiping-bcwipe-enterprise/).
  - DeleteOnClick (официальный сайт по адресу: http://www.2brightsparks.com/onclick/doc.html).
  - CyberShredder (официальный сайт по адресу: http://www.cylog.org/utilities/cybershredder.jsp).

4.2 Удаление критичных данных авторизации, сохранённых в процессе поиска неисправностей приложения (требование 1.1.5)

- У сервиса отсутствуют возможность сохранения каких-либо данных (данные ДДК и «чувствительные» данные) с целью отладки сервиса.

4.3 Удаление данных о держателях карт после истечения срока хранения этих данных, установленного пользователем (требование 2.1)

– У сервиса отсутствует возможность и необходимость сохранения данных о держателях карт (PAN) по какой-либо причине, поэтому необходимость в их удалении также отсутствует.

4.4 Защита ключей шифрования данных о держателях карт от неправомерного использования (требование 2.5)

– Сервис не хранит ключи и не использует их непосредственно. Все ключи хранятся только в криптоустройстве ПИН-клавиатура (EPP), являющимся сертифицированным на соответствие требованиям PCI DSS устройством.
– Необходимо использовать только ПИН-клавиатуры, сертифицированные на соответствие требованиям стандарта PCI DSS. Список сертифицированных ПИН-клавиатур опубликован на сайте Official PCI Security Standards Council Site на странице Approved PIN Transaction Security Devices по адресу: https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php# (см. Product Type / EPP и OEM EPP).

4.5 Реализация основных процедур управления ключами шифрования данных о держателях карт (требование 2.6)

– Для обмена сообщениями между платёжным сервисом и хостом процессинга могут использоваться 2 протокола: ISO8583 и IFX.
Используемый протокол устанавливается в файле настроек uniPayment-сервиса (**EFTPOS_Uniteller.ini**, секция [**Modules**], раскомментировать парамет **Protocol=IFXProtocol.dll** или **Protocol=SecureISOProtocol.dll** для работы по протоколу IFX или ISO8583 соответственно).
– Если выбран протокол ISO8583, то функции управления ключами шифрования данных о держателях карт uniPayment-сервисом не поддерживаются. Управление ключами шифрования осуществляется эквайером с помощью внешних инструментов при непосредственном доступе к ПИН-клавиатуре.
– При использовании IFX-протокола сервис поддерживает функцию автоматического обновления ключей шифрования путём запроса к серверу хоста и получения новых ключей в виде криптограмм, зашифрованных мастер-ключом. При этом дополнительные настройки сервиса не требуются. Процедура прошивки мастер-ключа производится эквайером с помощью внешнего инструмента при непосредственном доступе к ПИН-клавиатуре.

4.6 Удаление криптографических ключей и зашифрованных данных, сохранённых предыдущими версиями приложения (требование 2.7)

– Ключи в сервисе не хранятся, поэтому отсутствует необходимость удаления криптографических данных предыдущих версий сервиса.
– Необходимость в хранении каких-либо зашифрованных данных сервисом отсутствует.

4.7 Использование уникальных идентификаторов пользователей и безопасной аутентификации для административного доступа и доступа к данным о держателях карт (требование 3.1)

– Какие-либо данные о держателях карт на сервисе не хранятся.
– У сервиса отсутствует интерфейс пользователя, поэтому механизм и возможность обращения к сервису за получением данных отсутствует. Понятие идентификации пользователя к работе сервиса не применимо.

4.8 Использование уникальных идентификаторов пользователей и безопасной аутентификации для доступа к рабочим станциям, серверам и базам данных (требование 3.2)

– Платёжный uniPayment-сервер работает в системе платёжного терминала и не предусматривает отдельного удалённого доступа.
– Сервис в своей работе не использует никаких баз данных — только обращения к хосту эквайера, который, в свою очередь, сертифицирован на соответствие требованиям PCI DSS.
– В соответствии с требованиями п. 8 стандарта PCI DSS «Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре» для каждого терминала сети терминалов должны быть выполнены следующие условия:
  • Каждому пользователю должно быть назначено уникальное имя учётной записи до предоставления ему доступа к компонентам системы.
  • Помимо идентификатора, должен применяться хотя бы один из следующих методов для аутентификации всех пользователей:
    ○ То, что вы знаете (пароль и парольная фраза).
    ○ То, что у вас есть (ключи или смарт-карты).
    ○ То, что вы есть (биометрические параметры).
–
–

4.9 Внедрение автоматического журналирования событий (требование 4.1)

– Для выполнения требований пп. 10.1, 10.2 PCI DSS, которые требуют контролировать и отслеживать любой доступ к сетевым ресурсам и данным приложения, на терминале должен быть включён аудит средствами ОС терминала любых запросов к папке, в которой расположены файлы uniPayment-сервиса.
– Для включения аудита на ОС Windows (пример для английской версии) выполните следующие действия:

1. Откройте консоль управления политиками безопасности (**Start** > **Control Panel** > **Administrative Tools** > **Local Security Policy**) или выполните команду (**Start** > **Run…**) **SECPOL.MSC**.
2. В окне консоли в дереве политик выберите раздел **Audit Policy**, а справа в области значений свойство **Audit object access** и сделайте по нему двойной щелчок.
3. В открывшемся окне на вкладке **Local Security Setting** в области **Audit these attempts** установите галочку напротив значения **Saccess** и нажмите [**OK**].
4. Откройте окно свойств папки, в которой установлен uniPayment-сервис. Для этого в файловом менеджере выделите папку, в которой находится файл **EFTPOSUnitellerSrv.exe**, откройте контекстное меню и щёлкните пункт **Properties**.

5. В открывшемся окне перейдите на вкладку **Security** и нажмите кнопку [**Advanced**].
6. В открывшемся окне перейдите на вкладку **Auditing** и нажмите кнопку [**Add…**].
7. В открывшемся окне **Select User, Computer, or Group** убедитесь в том, что в поле **Select this object** выбрано значение **Built-in security principal**, если нет, то нажмите кнопку [**Object Types…**] и в открывшемся окне оставьте галочку только напротив значения **Built-in security principals**, нажмите [**OK**].
8. В поле ввода **Enter the object name to select** введите значение **Everyone**. Нажмите [**OK**].
9. В открывшемся окне Auditing Entry for <имя папки> в выпадающем списке Apply onto: выберите значение This folder, subfolders and files. В области Access: в столбце Successful установите галочки напротив пунктов: Create Files / Write Data, Delete, Delete Subfolders and Files, Change Permissions. Нажмите [OK].
10. Закройте открытые окна, нажимая [**OK**].

– Для включения аудита в ОС семейства Linux выполните следующие действия:

1. В файл по адресу **/etc/audit/audit.rules** добавьте строку:

```
-w /<папка, в которой расположен uniPayment-сервис>/ -p wa
```

2. Сохраните изменения и закройте файл.
3. Журнал аудита располагается по адресу **/var/log/audit**.

4.10 Включение данных журнала платёжного сервиса в централизованный лог сервера (требование 4.4)

– Так как решение об успешности авторизации и осуществление последующей финансовой транзакции (settlement) выполняются на хосте, их централизованное логирование и анализ ведутся на сервере хоста. Поэтому централизованное хранение логов на уровне платёжного сервиса не требуется.
– Логи платёжного сервиса направлены на отслеживание работы сервиса в штатном режиме, хранятся в папке, указанной в параметре **log_folder** конфигурационного файла сервиса, и являются текстовыми файлами. При необходимости эти файлы могут быть беспрепятственно скопированы на сервер централизованного хранилища логов мерчанта.
– При необходимости приведения формата записи логов платёжного сервиса к требуемому формату, это может быть осуществлено внешней утилитой, установленной на сервере логирования (по дополнительному согласованию с мерчантом).

4.11 Использование только необходимых и безопасных услуг, протоколов, компонент, программного и аппаратного обеспечения, в том числе предоставляемых третьими сторонами (требование 5.4)

– Для обмена сообщениями между платёжным сервисом и хостом процессинга могут использоваться 2 протокола: ISO8583 и IFX. Используемый протокол устанавливается в конфигурационном файле.
– При выборе работы по ISO8583-протоколу, транспортным протоколом является TCP, а безопасность передачи данных обеспечивается средствами, указанными в п. 2 «Общие требования для обеспечения безопасного использования uniPayment-сервиса» на стр. 6.
– При использовании IFX-протокола в качестве транспортного протокола используется защищённый протокол HTTPS.

– Использование каких-либо других транспортных протоколов должно быть исключено.

4.12 Безопасное использование при наличии беспроводных технологий (требование 6.1)

– При использовании беспроводных технологий для обеспечения связи терминалов с установленным uniPayment-сервисом, настройки беспроводного доступа должны быть осуществлены в соответствии с требованием п. 2.1.1 PCI DSS. Для этого все следующие настройки для беспроводных устройств, установленные производителем по умолчанию, должны быть изменены, а именно:
  - Ключи шифрования должны быть изменены при инсталляции и изменяться каждый раз, когда кто-либо, обладающий данными о ключах, уходит из компании либо переходит на другую должность.
  - Должны быть изменены установленные по умолчанию строки доступа SNMP беспроводных устройств.
  - Должны быть изменены установленные по умолчанию пароли/парольные фразы точек доступа.
  - Программное обеспечение беспроводных устройств должно быть обновлено до актуальной версии и поддерживать стойкие криптографические алгоритмы для аутентификации и передачи данных через беспроводные сети.
  - Также должны быть изменены любые другие настройки безопасности беспроводных устройств, установленные производителем по умолчанию.
– Также должны быть выполнены требования, изложенные в п. 2 «Общие требования для обеспечения безопасного использования uniPayment-сервиса» на стр. 6.

4.13 Безопасная передача данных платёжных карт по беспроводным сетям (требование 6.2)

– При использовании беспроводных технологий для передачи данных платёжных карт клиент должен использовать защищённый канал связи с помощью организации VPN-туннеля с использованием стойкого криптографического алгоритма.
  Для обеспечения безопасной передачи данных платёжных карт по беспроводным сетям должны быть выполнены требования, изложенные в п. 2 «Общие требования для обеспечения безопасного использования uniPayment-сервиса» на стр. 6.

4.14 Защита систем, хранящих критические данные, от проникновения из Интернета (требование 9.1)

– В работе сервиса не предусмотрена возможность хранения каких-либо данных о держателях карт или чувствительных данных, поэтому специальные мероприятия по защите этих данных от проникновения из Интернета не требуются.

4.15 Применение двухфакторной аутентификации для удалённого доступа к сервису (требование 10.2)

– Возможность прямого удалённого доступа к сервису отсутствует.
– Так как сервис работает в составе терминала, администратору терминала следует обеспечить доступ к терминалу с использованием уникальных идентификаторов и паролей, а также обеспечить уровень безопасности процесс авторизации не ниже уровня ОС семейства Windows.

4.16 Обеспечение безопасности при обновлении сервиса (требование 10.3.1)

– Обновление сервиса осуществляется только вручную при непосредственном доступе к терминалу. Обновление осуществляется путём замены файлов предыдущей версии сервиса файлами новой версии. Для обеспечения безопасности при обновлении сервиса необходимо получать файлы новой версии сервиса только из официального источника — на FTP-сервере Службы технической поддержки компании Uniteller.
– Процесс обновления uniPayment-сервиса включает в себя следующие этапы:

1. Проверка факта публикации более поздней, чем установленная, версии сервиса и принятие решения о необходимости обновления.
2. Загрузка последней версии сервиса с официального ресурса Uniteller.
3. Обновление установленного сервиса на последнюю версию.

– Для того чтобы узнать версию установленного uniPayment-сервиса выполните следующие действия:
  • В ОС Windows перейдите в папку с файлом установленного сервиса, откройте окно свойств файла **EFTPOSUnitellerSrv.exe** (выделите файл в файловом менеджере и нажмите **Alt+Enter** или пункт **Properties** в контекстном меню) и перейдите на вкладку «**Version**» — номер версии указан в поле «**File version:**».
  • В ОС Linux в меню запуска программ перейдите в раздел **Wine** и запустите **Проводник** (или выполните в Терминале команду **wine explorer**). Дальше действуйте аналогично работе в ОС Windows, как описано в предыдущем подпункте.

– Для того чтобы узнать номер последней опубликованной версии сервиса на официальном ресурсе Uniteller и, при необходимости, загрузить файл, выполните следующие действия:

1. Откройте страницу FTP-сервера Службы поддержки Uniteller, на которой размещены ссылки на последнюю версию файлов, входящих в пакет uniPayment-сервиса. Для этого откройте в браузере страницу с адресом: ftp://vss.unitecsys.com/helpdesk (для доступа на страницу используйте логин: eftpos и пароль: neweftpos).
2. Перейдите в папку с названием вида **Service X.X.X.X** . Номер текущей версии, история выпущенных версий и сделанных в них изменений перечислены в файле **Changes.txt**.
3. Примите решение о необходимости делать обновление (если у вас установлена последняя доступная версия сервиса, то обновление не требуется).
4. При необходимости обновления загрузите на диск локального компьютера файл последней версии uniPayment-сервиса (файл **EFTPOSUnitellerSrv.exe**).
5. Запросите у Службы технической поддержки Uniteller (по телефону 8 800 100 19 60 или электронной почте support@uniteller.ru) значение MD5-hash по содержимому файла **EFTPOSUnitellerSrv.exe** и, при необходимости, утилиту md5.exe, с помощью которой это значение можно вычислить.
6. Вычислите значение MD5-hash для скаченного файла и сверьте его со значением, полученным от Службы технической поддержки Uniteller. Если значения совпали — продолжите процесс обновления. Если значения не совпали, то сообщите об этом Службе

технической поддержки Uniteller и прервите процесс обновления.

– Для обновления сервиса выполните следующие действия:

1. Остановите запущенный uniPayment-сервис, для чего:
   - В среде Windows откройте окно **Run** (**Start** > **Run…**) и выполните команду:

```
<полный путь расположения файла EFTPOSUnitellerSrv.exe> -s
```

   - В среде Linux активизируйте запущенную через **Wine cmd-консоль** и в ней выполните аналогичную команду:

```
<полный путь расположения файла EFTPOSUnitellerSrv.exe> -s
```

2. Переместите загруженный файл **EFTPOSUnitellerSrv.exe** последней версии сервиса в папку, где установлен комплект файлов uniPayment-сервиса, заменив им имеющийся файл устаревшей версии.
3. Запустите uniPayment-сервис в работу, выполнив команду (аналогично с остановкой сервиса, описанного выше):

```
<полный путь расположения файла EFTPOSUnitellerSrv.exe> -r
```

4.17 Обеспечение безопасности использования ПО для удалённого доступа к сервису (требование 10.3.2)

– В штатном режиме работы платёжного сервиса отсутствует необходимость использования программ удалённого доступа. Однако, при необходимости, клиент может использовать программы удалённого доступа для организации доступа к своим терминалам при соблюдении требований п. 10.3.2 PA-DSS.

4.18 Шифрование данных при их передаче по общедоступным сетям (требование 11.1)

– Для передачи данных между платёжным сервисом и хостом процессинга необходимо использовать шифрованные каналы связи типа VPN-туннеля с использованием стойкого криптографического алгоритма.
Для обеспечения безопасной передачи данных платёжных карт по общедоступным сетям должны быть выполнены требования, изложенные в п. 2 «Общие требования для обеспечения безопасного использования uniPayment-сервиса» на стр. 6.

4.19 Обеспечение безопасности передачи данных платёжных карт при использовании технологий обмена сообщениями между конечными пользователями (требование 11.2)

– Так как сервис работает локально на терминале клиента, то никакие технологи обмена сообщениями с конечным клиентом не требуются. Клиент вводит ПИН-код непосредственно

на шифрующем устройстве (ПИН-клавиатуре), а данные платёжных карт получаются путём считыванием карты в считывающем устройстве терминала.

- Необходимым условием является подключение ПИН-клавиатуры и считывателя карт непосредственно к терминалу, на котором установлен uniPayment-сервис.

4.20 Шифрование неконсольного административного доступа (требование 12.1)

- uniPayment-сервис не поддерживает функцию неконсольного доступа к себе.
- Если ПО терминала предоставляет возможность неконсольного доступа к терминалу, а также предоставляет возможность посредством своего интерфейса управлять uniPayment-сервисом, то в этом случае реализация неконсольного доступа к терминалу должна реализовываться с соблюдением требований п. 2.3 PCI DSS.