



SmartCard-Service

Акционерное общество «СмартКарт-Сервис»

127106, г. Москва, Алтуфьевское шоссе, д. 1

Телефон: +7 (495) 981-12-10, 8 (800) 100-31-64, факс: +7 (495) 981-12-11

E-mail: reception@scserv.ru, site: www.scserv.ru

УТВЕРЖДЕНО

Генеральный директор

_____ В.А. Васильев

«_____» _____ 20__ г.

Программное обеспечение для устройств самообслуживания «TelME 7»

9. Руководство по применению стандарта PA-DSS ver. 3.2

Дата внесения изменений: 18.08.2021 13:26:35

Файл: tellme7_09_руководство по применению стандарта pa-dss ver_3_2.docx

Москва
2021

СОДЕРЖАНИЕ

1. Сведения о документе.....	4
2. Введение	4
3. Список терминов и сокращений	4
4. Общая информация.....	5
5. Деинсталляция и возврат ПО «TellME» предыдущих версий.....	6
5.1. Деинсталляция ПО «TellME» предыдущих версий	6
5.2. Процедуры возврата ПО «TellME» предыдущих версий.....	6
6. Инсталляция и ввод в эксплуатацию ПО «TellME 7».....	7
6.1. Инсталляция ПО «TellME 7» базовой версии	7
6.2. Инсталляция Обновлений ПО «TellME 7»	7
6.2.1. Инсталляция обновлений	8
6.2.2. Удаленная инсталляция обновлений	8
7. Удаление и шифрование критичных данных	10
7.1. Маскирование данных платежных карт	10
7.2. Шифрование данных платежных карт	10
7.3. Безопасная трассировка буферов транзакций NDC.....	11
7.4. Удаление карточных данных после работы ПО «TellME 7» в тестовом режиме	11
8. Защита данных платежных карт при хранении	13
8.1. Хранение данных платежных карт в журналах.....	13
8.2. Безопасное управление ключами шифрования, хранящимися в EPP-клавиатуре	15
8.3. Клавиатуры, с которыми ПО «TellME 7» работает в соответствии с требованиями стандарта PA-DSS	15
9. Удаление ключей шифрования предыдущих версий	17
10. Настройка доступа	17
11. Журналы аудита.....	18
11.1. Резервное копирование журналов аудита	18
12. Использование протоколов и сервисов.....	19
13. Использование беспроводных технологий.....	19
14. Обеспечение защиты среды эксплуатации	20
15. Удаленный доступ	20
16. Передача данных платежных карт по сетям общего пользования	22
17. Неконсольный административный доступ.....	22
18. Дополнительные возможности отладки в тестовом режиме.....	22
18.1. Формирование данных RMS-журнала	22
18.2. Конфигурация для приема карт стандарта «EMV».....	23
19. ПО сторонних производителей	23
20. Версии и модификации	24
21. История изменений документа	28

1. СВЕДЕНИЯ О ДОКУМЕНТЕ

Номер версии:	01.00
Дата выпуска:	18.08.2021 г.
Дата утверждения:	
Порядок обновления:	— 1 раз в год; — при обновлении ПО «TellME 7» (при необходимости); — при обновлении стандарта PCI DSS и PA-DSS

2. ВВЕДЕНИЕ

Настоящий документ является частью организационного обеспечения разработки ПО «TellME 7». В документе «Руководство по применению стандарта PA-DSS» (далее — Руководство) содержатся инструкции по настройке дополнительной защиты программного продукта в соответствии со стандартом PA-DSS, четкое определение обязанностей производителя, дилеров/системных интеграторов и клиентов для достижения соответствия с требованиями стандарта PCI DSS. В Руководстве содержатся подробные сведения о том, какие параметры безопасности должен выбрать клиент и/или дилер/системный интегратор.

В Руководстве приведены обязанности сторон по реализации требований, указанных в стандарте PA-DSS. Документ содержит 28 страниц.

3. СПИСОК ТЕРМИНОВ И СОКРАЩЕНИЙ

Сокращение	Расшифровка
PA-DSS	Стандарт безопасности данных платежных приложений индустрии платежных карт (Payment Application Data Security Standard)
PCI DSS	Стандарт безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard)
ПО	Программное обеспечение
ПО «TellME 7»	Программное обеспечение для устройств самообслуживания «TellME 7»
УС	Устройство самообслуживания
ПК	Персональный компьютер
ПМ	Программный модуль
ОС	Операционная система
МЭ	Межсетевой экран

Сокращение	Расшифровка
Надежная криптография	<p>Основное определение криптографии, которое является чрезвычайно значимым для криптоанализа. Т.е. зная криптографический метод (алгоритм или протокол) невозможно получить криптографический ключ или зашифрованные данные. Надежность определяется использованием криптографических ключей. Для наибольшей эффективности размер ключа должен исходить из минимального размера ключа соизмеримого с рекомендуемым уровнем защиты. Минимальный уровень защиты можно определить из NIST Специальной Публикации 800-57, Август, 2005 (http://csrc.nist.gov/publications/) или иначе, в соответствии с представленным далее минимальным набором бит для обеспечения безопасности ключа:</p> <ul style="list-style-type: none">• 80 битов для секретного ключа базовой системы (например, TDES) при условии, что первый и третий ключ при шифровании данных по алгоритму 3DES будут равны, эффективная длина ключа будет 80 бит, однако, фактическая длина ключа – 112 бит;• 2048 битовый модуль для открытых алгоритмов ключей, основанных на факторизации (например, RSA);• 2048 бита для дискретного логарифма (например, Diffie-Hellman) с минимальным размером 256 бит основной подгруппы (например, DSA);• 160 бит для криптографии по эллиптической кривой (например, ECDSA)

4. ОБЩАЯ ИНФОРМАЦИЯ

Предлагаемые способы учитывают необходимость соблюдения требований стандартов безопасности в индустрии платежных карт, разработанных международными платежными системами «Visa» и «MasterCard»: Стандарта безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard, PCI DSS) и Стандарта безопасности данных платежных приложений индустрии платежных карт (Payment Application Data Security Standard, PA-DSS).

Название программного обеспечения — «TellME 7».

Версия программного обеспечения — 02.00.

Программное обеспечение должно быть настроено согласно настоящему документу «Руководство по применению стандарта PA-DSS».

Обновленные версии документа «Руководство по применению стандарта PA-DSS» предоставляются клиентам Компании, использующим программное обеспечение ПО «TellME 7».

Отметки о доработках документа «Руководство по применению стандарта PA-DSS» вносятся в таблицу, приведенную в разделе «21. История изменений документа».

5. ДЕИНСТАЛЛЯЦИЯ И ВОЗВРАТ ПО «TELLME» ПРЕДЫДУЩИХ ВЕРСИЙ

5.1. Деинсталляция ПО «TellME» предыдущих версий

Установка новой версии ПО для устройств самообслуживания «TellME 7» должна осуществляться с обязательной предварительной деинсталляцией предыдущей версии.

Удаление предыдущей версии ПО для устройств самообслуживания «TellME» выполняется штатными средствами Windows «Start» => «Settings» => «Control Panel» => «Add/Remove Programs» вкладка «Install/Uninstall». Удалите ПО «TellME» => «SCS_TellME».

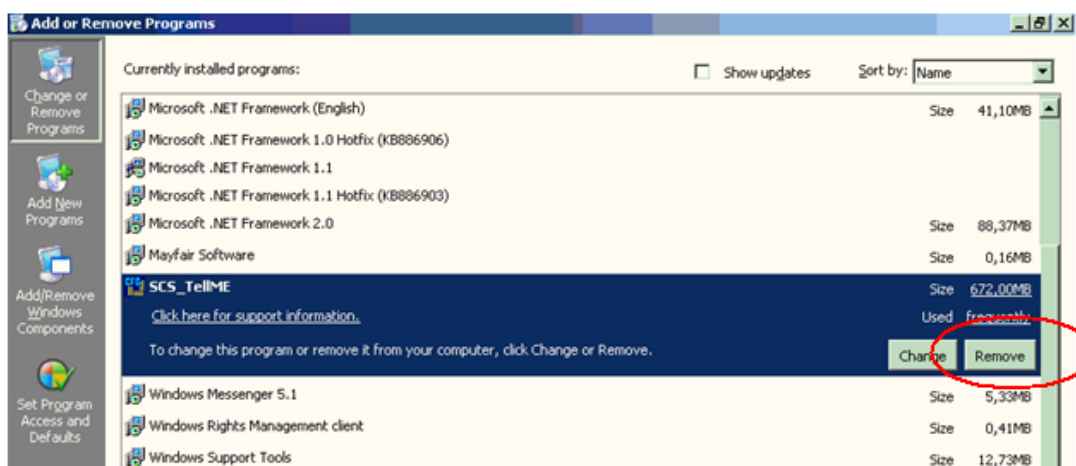


Рис. 1. «Start» => «Settings» => «Control Panel» => «Add/Remove Programs»

Далее удалите нижеперечисленные данные безопасным способом, например, с помощью программы «SDelete», которая доступна на сайте компании Microsoft (безопасный способ подразумевает удаление данных без возможности их восстановления):

- 1) директорию C:\SCS;
- 2) аппаратные журналы C:\SCS\LOGS\ERL*.ERL;
- 3) файлы обмена данными между процессами C:\SCS\PRIVATEDATA\scsmem.dll\SCS_HEAP.mem или C:\SCS\PRIVATEDATA\scsmem.dll\SCSSHARE.mem (при установке по умолчанию);
- 4) неиспользуемые области диска.

5.2. Процедуры возврата ПО «TellME» предыдущих версий

ПО «TellME» не предоставляет собственные процедуры возврата ПО предыдущих версий.

Для восстановления предыдущей версии ПО, необходимо удалить текущую версию (см. раздел текущего документа «5.1. Деинсталляция ПО «TellME» предыдущих версий»), затем установить предыдущую версию программного обеспечения «TellME» (см. соответствующий раздел эксплуатационной документации к ПО «TellME»).

6. ИНСТАЛЛЯЦИЯ И ВВОД В ЭКСПЛУАТАЦИЮ ПО «TELLME 7»

6.1. Установка ПО «TellME 7» базовой версии

Для установки базовой версии ПО «TellME 7» необходимо предварительно выполнить форматирование на низком уровне жесткого диска УС, на который в дальнейшем будет выполнена установка ОС Windows, программно-аппаратного уровня от производителя (при необходимости) и ПО «TellME 7». Затем безопасно сотрите неиспользуемые области диска (например, с помощью программы «SDelete»).

Установку ПО «TellME 7» следует производить пользователю с правами администратора.

Подробная процедура установки ПО «TellME 7» описана в документе «Руководство по установке», входящего в комплект документации к ПО «TellME 7», процедура конфигурирования конкретного УС и специфические настройки для его работы отражены в документе «Руководство по настройке».

Внимание!

При наличии в дистрибутивном комплекте кроме базовой версии ПО «TellME 7» еще и Обновления, установка Обновления производится сразу после установки базовой версии ПО «TellME 7» без его запуска.

Для работы с пользователями системы в ОС **Windows 10 (Windows 10 IoT Enterprise LTSC 2016 (v.1607), Windows 10 IoT Enterprise LTSC 2019 (v.1809)), Windows 7 (Windows Embedded POSReady 7) и Windows XP (Windows Embedded POSReady 2009)** измените значение параметра «Accounts: Rename administrator account» с «Administrator» на любое другое произвольное имя (т.е. переименуйте пользователя «Administrator» на любое другое произвольное имя).

Удаление пользователя «Guest» системой запрещено, поэтому отключите его учетную запись, изменив значение «Accounts: Guest account status» на «Disabled».

Далее произведите настройки политики безопасности ОС Windows в соответствии с требованиями стандарта PA-DSS пользователем, имеющим на этом компьютере права администратора (см. документ «Утилита "TellME Advanced Security". Руководство по установке и настройке», раздел «Настройка политики безопасности ОС самостоятельно»).

Те же самые настройки можно выполнить автоматически с помощью инсталлятора «TellME Advanced Security» (лицензионная компонента приобретается отдельно). Особенности установки «TellME Advanced Security» описаны в документе «Утилита "TellME Advanced Security". Руководство по установке и настройке», в разделе «Установка утилиты "TellME Advanced Security"». После этого выполните дополнительные настройки политики аудита в соответствии с рекомендациями, приведенными в разделе «11. Журналы аудита» настоящего документа.

6.2. Установка Обновлений ПО «TellME 7»

Компания АО «СмартКарт-Сервис» периодически выпускает Обновления к ПО «TellME 7».

Выпуск каждой версии (релиз) сопровождается оповещением всех заинтересованных лиц.

Выпущенные Обновления к ПО «TellME 7» размещаются на портале объединенного сервисного центра АО «СмартКарт-Сервис» по адресу <https://support.scserv.ru>.

Для получения Обновления клиенту, зарегистрированному в Системе Сопровождения Клиентов, необходимо войти на портал под своей учетной записью, выбрать пункт меню «Центр загрузки», в появившемся списке выбрать нужный раздел и из него скачать необходимый архив с Обновлением.

В состав Обновления ПО «TellME 7» входит файл **checksum.sha256**, в котором содержится список хеш-сумм файлов, входящих в дистрибутивный комплект.

После скачивания архива Обновления ПО «TellME 7» необходимо проверить целостность каждого файла, включенного в архив. Целостность файлов можно проверить любой программой, которая подсчитывает хеш-сумму по алгоритму SHA-256.

При несовпадении хеш-сумм необходимо обратиться в Службу сопровождения АО «СмартКарт-Сервис».

Также архив Обновления ПО «TellME 7» содержит документ «Release Notes», в котором указывается номер новой версии ПО «TellME 7» и список основных изменений в версии.

6.2.1. Установка обновлений

Компания АО «СмартКарт-Сервис» периодически выпускает Обновления к ПО «TellME 7», Порядок установки обновлений приводится в эксплуатационной документации для соответствующего Обновления.

Внимание!

При наличии в дистрибутивном комплекте кроме базовой версии ПО «TellME 7» еще и Обновления, установка Обновления производится сразу после установки базовой версии ПО «TellME 7» без его запуска.

6.2.2. Удаленная установка обновлений

Удаленный доступ к ПК устройства самообслуживания и установка обновлений ПО «TellME 7» осуществляется клиентами или дилерами/системными интеграторами самостоятельно.

Если обновление производится с помощью удаленного доступа, то удаленный доступ необходимо включать только при загрузке обновлений производителя и отключать его сразу после завершения загрузки. Альтернативный вариант — при получении обновления с помощью VPN-подключения или другого высокоскоростного подключения, необходимо использовать межсетевые экраны с целью надежной защиты этих постоянных соединений.

Также для удаленных подключений должна быть использована двухфакторная аутентификация.

Для соответствия требованиям **п.1 стандарта PCI DSS** должны быть реализованы стандарты конфигурирования межсетевых экранов (МЭ) и маршрутизаторов, включающие следующее:

- Формальный процесс утверждения и тестирования всех подключений сетей, а также изменений, вносимых в конфигурацию МЭ.
- Актуальную схему сети с указанием всех подключений (включая беспроводные сети) к сегментам с данными платежных карт.

- Требования по размещению МЭ на каждом канале подключения к сети Интернет, а также на границе между каждой DMZ и внутренней сетью.
- Описание групп, ролей и обязанностей в отношении логического управления сетевыми компонентами.
- Документирование и обоснование применения для всех использующихся сервисов, протоколов и портов, включая документирование реализованных механизмов защиты для небезопасных протоколов.
- Пересмотр наборов правил МЭ и маршрутизаторов не реже, чем через каждые 6 месяцев.

Должна быть реализована такая конфигурация МЭ, которая ограничивает возможность подключения недоверенных сетей к системным компонентам среды данных платежных карт.

Внимание!

Под недоверенной сетью понимается любая сеть, которая является внешней по отношению к сетям проверяемой организации. Организация не может контролировать такую сеть и управлять ею.

- Разрешение только такого входящего и исходящего трафика, который является необходимым для среды данных платежных карт.
- Обеспечение защиты и синхронизации конфигурационных файлов маршрутизаторов.
- Установка МЭ для организации защиты периметра между любыми беспроводными сетями и средой платежных карт и конфигурирование этих МЭ на блокирование любого трафика из беспроводных сетей в среду данных платежных карт или контроль этого трафика (если такой трафик необходим для ведения бизнеса).

Должен быть запрещен любой доступ из сети Интернет к любым системным компонентам среды данных платежных карт.

- Должна быть реализована зона DMZ для ограничения входящего и исходящего трафика только теми протоколами, которые необходимы для среды данных платежных карт.
- Входящий интернет-трафик должен быть ограничен IP-адресами внутри DMZ.
- Запрет прямой маршрутизации входящего или исходящего трафика между сетью Интернет и средой данных платежных карт.
- Запрет трафика с адресами отправителя внутренней сети, поступающего в DMZ из сети Интернет.
- Ограничение трафика исходящего из среды данных платежных карт в Интернет, таким образом, чтобы исходящему трафику были доступны только IP-адреса в пределах демилитаризованной зоны (DMZ).
- Реализация фильтрации трафика с учетом состояния соединений (stateful inspection), также известной как динамическая фильтрация пакетов (когда доступ в сеть разрешается только для «установленных» соединений).
- Размещение базы данных во внутреннем сегменте сети, отделенном от DMZ.
- Для предотвращения трансляции и раскрытия внутренней адресации в сети Интернет должно осуществляться сокрытие IP адреса источника сообщения с использованием адресного пространства частных сетей (RFC 1918). Должны использоваться технологии

преобразования сетевых адресов (NAT), например, технология переназначения портов и адресов (PAT).

Установка персональных межсетевых экранов на все портативные и/или личные компьютеры сотрудников, которые обладают возможностью прямого доступа к сети Интернет (например, на ноутбуки сотрудников) и используются для доступа к сети организации.

7. УДАЛЕНИЕ И ШИФРОВАНИЕ КРИТИЧНЫХ ДАННЫХ

Для минимизации рисков в ПО «TellME 7» требуется хранение минимального набора критичных данных карты, которые необходимы для ведения бизнеса. Для работы ПО «TellME 7» необходимо хранить следующие элементы:

- Номер платежной карты (PAN).

В программном обеспечении отображение номера PAN платежных карт представляется в маскированном виде.

7.1. Маскирование данных платежных карт

ПО «TellME 7» маскирует номера платежных карт (PAN):

- в журнал PRJ и титры системы видеонаблюдения записывается номер PAN платежной карты в маскированном виде;
- в журналах *.XML маскирование данных производится по алгоритму аналогично записи в журнал PRJ;
- в журнал PRJ дополнительно записывается значение HASH, вычисляемое по алгоритму SHA1, от значений DateTime, TerminalID и PAN платежной карты.

Внимание!

Использование библиотеки отличной от C:\SCS\Atm_h\CustCardDSS.dll может привести к нарушению требований *PCI DSS* и *PA-DSS*.

В журналах платежных систем, работающих по протоколу ISO-8583, процессе в проведения транзакции хранится только маскированный номер PAN в директории C:\SCS\LOGS\<Наименование платежной системы>\.

7.2. Шифрование данных платежных карт

В процессе проведения транзакции для обмена данными между процессами формируются файлы C:\SCS\PRIVATEDATA\scsmem.dll\SCS_HEAP.mem и C:\SCS\PRIVATEDATA\scsmem.dll\SCSSHARE.mem (при установке по умолчанию), в которых, в том числе, могут содержать критичные данные. Данные в файлах шифруются по алгоритму 3DES на базе динамически генерируемых ключей (длиной 16 байт). После окончания транзакции данные надежным способом удаляются, ключи уничтожаются.

В процессе прохождения авторизации по протоколу ISO-8583 ПО «TellME 7» создает файл в директории C:\SCS\ATM_H\specdata>LastOper_<Наименование платежной системы> с зашифрованными данными PAN (которые используются для отмены транзакции в случае перезапуска программного обеспечения). PAN и данные транзакций шифруются с помощью алгоритма 3DES на базе динамически генерируемых ключей (длиной 16 байт). После окончания транзакции данные надежным способом удаляются, ключи уничтожаются.

Для идентификации клиентов во внешних системах может использоваться HASH номера карты, вычисленный по алгоритму SHA256. В этом случае во внешние системы передается только значение HASH без каких-либо дополнительных карточных данных.

Внимание!

Использование библиотеки отличной от C:\SCS\Atm_h\CustCardDSS.dll может привести к нарушению требований *стандарта PCI DSS* и *PA-DSS*.

7.3. Безопасная трассировка буферов транзакций NDC

Журналы платежной системы NDC/NDC2 (*.NDC) в директории C:\SCS\LOGS\NDC\NDC\ или C:\SCS\LOGS\NDC2\NDC\ содержат данные, передаваемые между сервером платежной системы NDC/NDC2 и УС. Данные платежных карт, передаваемые с сервера, должны быть представлены в нечитаемом виде.

Для маскирования данных в печатном буфере NDC/NDC2 необходимо воспользоваться ESC-последовательностями:

[ESC:Э] — включить режим маскирования;

[ESC:Ю] — выключить режим маскирования.

Если пользователи ПО «TellME 7» (при использовании платежной системы NDC) изменяют содержимое стандартных буферов транзакции (Buffer B, Buffer C), то для соответствия требованиям *стандарта PA-DSS* необходимо отключить трассировку буферов, содержащих критические данные. Для этого необходимо в сценарий платежной системы NDC/NDC2 добавить стейт f-027 (Стейт изменения режима трассирования буферов транзакции). Описание данного стейта находится в документации «Платежная система NDC», входящей в состав комплекта документации ПО «TellME 7».

Данные Buffer B и/или Buffer C будут замаскированы в журналах C:\SCS\LOGS\NDC\NDC\YYYYMMDD.NDC или C:\SCS\LOGS\NDC2\NDC\ YYYYMMDD.NDC и C:\SCS\LOGS\NDC\STF\YYYYMMDD.STF или C:\SCS\LOGS\NDC2\STF\YYYYMMDD.STF.

7.4. Удаление карточных данных после работы ПО «TellME 7» в тестовом режиме

Во время работы ПО «TellME 7» в тестовом режиме (с использованием тестового ключа лицензионной защиты) карточные данные и критические данные сохраняются в электронных журналах ПО «TellME 7» в директориях c:\scs\logs\ и c:\scs\logs_archive\.

После эксплуатации ПО «TellME 7» в тестовом режиме должно быть выполнено удаление карточных данных и критических данных безопасным способом (безопасный способ подразумевает удаление данных без возможности их восстановления).

Для безопасного гарантированного удаления карточных данных и критических данных во время работы ПО «TellME 7» в тестовом режиме необходимо следовать следующим рекомендациям.

1. Перед установкой тестового ключа лицензионной защиты (или обновления лицензии) во избежание потери данных необходимо скопировать или переместить на внешний носитель все файлы из директории c:\scs\logs\ и c:\scs\logs_archive\ (при установке по умолчанию).
2. Установить тестовый ключ лицензионной защиты (или обновить лицензию).
3. Провести тестовые операции и проанализировать поведение ПО «TellME 7».
4. После завершения тестовых операций заменить тестовый ключ лицензионной защиты на рабочий ключ лицензионной защиты.
5. Удалить средствами ОС директории c:\scs\logs и c:\scs\logs_archive\ (при установке по умолчанию).
6. Для безопасного гарантированного удаления карточных данных и критических данных, которые сохранились во время работы ПО «TellME 7» в тестовом режиме, воспользоваться утилитой «SDelete», которая доступна на сайте компании Microsoft по ссылке <https://docs.microsoft.com/ru-ru/sysinternals/downloads/sdelete>.

Пример.

Пример использования утилиты «SDelete» приведен ниже.

<Путь>SDelete.exe <Название диска, в нашем случае c:> -s -q -z -p 3, где

c: — название диска;

-s — включая подкаталоги;

-q — не выводить на экран ошибки («тихий» режим);

-z — провести очистку свободного места;

-p 3 — количество проходов перезаписи незаполненного пространства (рекомендуется три).

Внимание!

Тестовый режим реализован для использования и отладки работы ПО «TellME 7» в инфраструктуре клиента. Сотрудники компании АО «СмартКард-Сервис» не занимаются сбором, обработкой, анализом и консультированием пользователей по журналам (log-файлам), генерируемым в инфраструктурах клиентов в тестовом режиме с использованием тестового лицензионного ключа. Для соблюдения требований стандарта PA-DSS **категорически запрещается передача данных**, полученных в результате работы ПО «TellME 7» с тестовым лицензионным ключом.

8. ЗАЩИТА ДАННЫХ ПЛАТЕЖНЫХ КАРТ ПРИ ХРАНЕНИИ

Для соблюдения требований **PA-DSS** используемые данные платежных карт необходимо удалять после истечения срока их хранения. ПО «TellME 7» не хранит полные номера карт и критичные данные платежных карт после авторизации.

8.1. Хранение данных платежных карт в журналах

Журналы платежных систем ISO-протокола в директории C:\SCS\ATM_H\specdata>LastOper_<Наименование платежной системы>\ безопасно удаляются после завершения транзакции.

Информация в файлах C:\SCS\PRIVATEDATA\scsmem.dll\SCS_HEAP.mem и C:\SCS\PRIVATEDATA\scsmem.dll\SCSSHARE.mem затирается после завершения транзакции.

Внимание!

Для соблюдения требований PA-DSS по аудиту всех файлов, содержащих критичные данные, запрещается изменять расположение файлов C:\SCS\PRIVATEDATA\scsmem.dll\SCS_HEAP.mem и C:\SCS\PRIVATEDATA\scsmem.dll\SCSSHARE.mem.

В других журналах, создаваемых ПО «TellME 7», хранятся только номера платежной карты (PAN) в маскированном виде. При необходимости можно вручную удалить журналы из соответствующих директорий.

Внимание!

Использование библиотеки отличной от C:\SCS\Atm_h\CustCardDSS.dll может привести к нарушению требований стандарта PCI DSS и стандарта PA-DSS.

Электронные журналы ПО «TellME 7» в формате ГГГГММДД

Размещение электронных журналов	Тип и принадлежность электронных журналов
C:\SCS\LOGS\PRJ	Технические журналы (*.PRJ)
C:\SCS\LOGS\PRR	Журналы чеков (*.PRR)
C:\SCS\LOGS\ERL	Аппаратные журналы (*.ERL)
C:\SCS\LOGS\HWR	HWR-журналы (*.HWR)
C:\SCS\LOGS\XML_OD	Файл операционных циклов диспенсера (*.cdm.xml)
C:\SCS\LOGS\XML_OD	Файл операционных циклов модуля приема наличных (*.bim.xml)
C:\SCS\LOGS\XML	Файл операций (*.tran.xml)
C:\SCS\LOGS\NDC\ndc	Журналы платежной системы NDC (*.NDC)

Размещение электронных журналов	Тип и принадлежность электронных журналов
C:\SCS\LOGS\NDC2\ndc	Журналы платежной системы NDC2 (*.NDC)
C:\SCS\LOGS\NDC\EMV	Журналы EMV-ядра платежной системы NDC (*.EMV)
C:\SCS\LOGS\NDC2\EMV	Журналы EMV-ядра платежной системы NDC2 (*.EMV)
C:\SCS\LOGS\TK\	Журналы платежной системы Transmaster (*.batch_TK.IMA)
C:\SCS\LOGS\TK_PT\	Журналы платежной системы Transmaster_PT (*.batch_TK_PT.IMA)
C:\SCS\LOGS\OWMB\	Журналы платежной системы OpenWay (*.batch_OWMB.IMA)
C:\SCS\LOGS\OWMB_PT\	Журналы платежной системы OpenWay_PT (*.batch_OWMB_PT.IMA)
C:\SCS\LOGS\ZK\	Журналы платежной системы «Золотая Корона»
C:\SCS\LOGS\SVFE_TF\	Журналы платежной системы SVFE_TF
C:\SCS\LOGS\NFC	Журнал трассировки команд NFC-ридера (*.NFC)
C:\SCS\ATM_H\specdata\	LastOper_PG.dat
C:\SCS\ATM_H\specdata\	LastOper_PG_PT.dat
C:\SCS\ATM_H\specdata\	LastOper_TK.dat
C:\SCS\ATM_H\specdata\	LastOper_TK_PT.dat
C:\SCS\ATM_H\specdata\	LastOper_OWMB.dat
C:\SCS\ATM_H\specdata\	LastOper_OWMB_PT.dat
C:\SCS\PRIVATE\DATA\scsmem.dll\	SCS_HEAP.mem
C:\SCS\PRIVATE\DATA\scsmem.dll\	SCSSHARE.mem

Журналы платежных систем в директории C:\SCS\LOGS\<Наименование платежной системы>\ хранятся 30 дней.

По умолчанию срок хранения журналов ERL составляет 90 дней, PRJ, PRR — 180 дней. По истечении установленного срока журналы удаляются автоматически.

Перед запуском ПО «TellME 7» необходимо обязательно проверить параметры настройки срока хранения журналов в соответствующих ветках реестра:

[HKEY_LOCAL_MACHINE\SOFTWARE\SCS\Utilities\JournalFiles\ERL];

[HKEY_CLASSES_ROOT\WOSA\XFS_ROOT\ATM\PRJ];

[HKEY_CLASSES_ROOT\WOSA\XFS_ROOT\ATM\PRR]

параметр «HistoryDays»=dword — срок хранения журналов.

Для платежной систем NDC/NDC2 необходимо проверить параметры настройки срока хранения и количества журналов:

[HKEY_CLASSES_ROOT\WOSA\XFS_ROOT\ATM\PaymentSystems\NDC\Config\Channel]

или

[HKEY_CLASSES_ROOT\WOSA\XFS_ROOT\ATM\PaymentSystems\NDC2\Config\Channel]

параметр «MaxLogHistory»=dword:0000002d (45) — срок хранения журналов (45 дней);

параметр «MinLogFiles»=dword:0000000a (10) — количество журналов, не подлежащих удалению (10 последних файлов).

8.2. Безопасное управление ключами шифрования, хранящимися в EPP-клавиатуре

Платежное приложение не генерирует, не распространяет, не изменяет, не хранит и не уничтожает/изменяет криптографические ключи шифрования. Эти процедуры выполняются процессинговыми центрами клиентских организаций самостоятельно и должны соответствовать требованиям *PA-DSS*. Также должен быть предоставлен конверт с ключами шифрования и приняты процедуры предотвращения несанкционированной замены ключей.

Ключи для работы с данными платежных карт можно загрузить только в шифрованном виде. Приложение не хранит данные ключа на диске. Полученные данные передаются в модуль шифрования напрямую или через API, поставляемым с конкретным оборудованием.

Внимание!

Перед вводом ключей шифрования убедитесь, что прошивка EPP-клавиатуры соответствует требованиям PCI-DSS!

Доступ к криптографическим ключам должен быть предоставлен минимальному количеству сотрудников, которым он необходим. Для ограничения доступа персонала банка к вводу ключей шифрования АО «СмартКард-Сервис» рекомендуем воспользоваться утилитой «SCS_KeyLoader» (данная утилита позволяет создать пользователя с ограниченными правами). После ввода ключей шифрования необходимо удалить файл C:\SCS\TellMe\SCS_KeyLoader.txt, содержащий логин и пароль пользователя с ограниченными правами, и заблокировать пользователя с учетной записью «SCS_KeyLoader».

Кроме того, в модуль шифрования аппаратно все ключи загружаются в виде двух компонент. Это также позволяет исключить доступ сотрудников к реальному значению ключа.

Программное обеспечение «TellME 7» не хранит криптографические ключи. Все ключи хранятся в модуле шифрования.

Более подробное описание реализованных процессов и процедур приведено в документе «Шифрование и управление ключами».

8.3. Клавиатуры, с которыми ПО «TellME 7» работает в соответствии с требованиями стандарта PA-DSS

Ниже приведен список моделей клавиатур, с которыми ПО «TellME 7» работает в соответствии с требованиями стандарта PCI-DSS.

- XFS NCR (при установке прошивки PCI);
- XFS DIEBOLD OPTEVA (при установке прошивки PCI);
- XFS DIEBOLD OPTEVA v.6 (при установке прошивки PCI);
- Hyosung Nautilus (6000/8000);

- Wincor EPP v.5;
- Wincor EPP v.6;
- Wincor EPP v.7;
- Wincor EPP v.8;
- Cryptera (Sagem) 1217-5610 с прошивкой ver. 414-0697 R2E (имеет ограничение на ввод одного ключа шифрования);
- Cryptera (Sagem) 1217-5610 с прошивкой ver. 414-0697 R3A (не имеет ограничений на ввод ключей шифрования);
- Cryptera (Sagem) 1215-5610 с прошивкой ver. 414-0697 R2F (имеет ограничение на ввод одного ключа шифрования)
- Thales v.5 COM;
- Thales v.5 USB;
- Thales v.6 USB;
- ZT-588-CA7-D16;
- ZT-588-FA6-F20;
- ZT588-F46-F20;
- ZT-588-F46-F30
- ZT-596-E10-F17;
- ZT-596-F30-H40
- ZT596-NFG-H21
- ZT-596-E10-F17-SYS;
- ZT-596E-NE0-F20-ZZZ.02;
- ZT596F-NF0-H21-ZZZ.01;
- ZT-598-M5C-H12
- ZT-598-L5J-H50
- OKI;
- GRG XFS.

Внимание!

ПО «TellME 7» не удовлетворяет требованиям стандарта PA-DSS при работе с клавиатурой **ZT596F-NF0-H21-ZZZ.01 с библиотекой pinZTx1.dll** (не входит в дистрибутивный комплект ПО «TellME 7»!)

Внимание!

С клавиатурами, не перечисленными в данном разделе, ПО «TellME 7» работает без соответствия требованиям стандарта PCI-DSS. Следовательно, при работе с ними ПО «TellME 7» не будет удовлетворять требованиям стандарта PA-DSS!

9. УДАЛЕНИЕ КЛЮЧЕЙ ШИФРОВАНИЯ ПРЕДЫДУЩИХ ВЕРСИЙ

Ключи шифрования не хранятся на жестком диске УС и не требуют применения дополнительных процедур удаления.

Процесс деинсталляции ПО «TellME 7» включает в себя безвозвратное удаление всех компонентов системы, электронных журналов, параметров реестра и всех исторических данных (см. раздел «5. Деинсталляция и возврат ПО «TellME» предыдущих версий» настоящего документа).

10. НАСТРОЙКА ДОСТУПА

В ПО «TellME 7» существует один тип учетных записей пользователей. Данная учетная запись не имеет доступа к данным платежных карт и административных привилегий, влияющих на выполнение требований стандарта PA-DSS.

При входе в УС с установленным ПО «TellME 7» используется механизм аутентификации ОС Windows.

Управление учетными записями для доступа к УС осуществляется администратором ОС.

Пользователи ПО «TellME 7» не имеют доступа к данным платежных карт. Для настройки политики безопасности ОС Windows АО «СмартКарт-Сервис» разработан инсталлятор политики безопасности ОС Windows «TellME Advanced Security» или пользователь может самостоятельно произвести настройки в соответствии с требованиями стандарта PA-DSS, указанные в текущем разделе документа (подробнее (см. документ «Утилита “TellME Advanced Security”. Руководство по инсталляции и настройке», раздел «Настройка политики безопасности ОС самостоятельно»).

Для учетных записей, установленных на уровне ОС, необходимо настроить следующие атрибуты парольной политики:

- использовать персональные учетные записи, запретить использование групповых учетных записей и паролей;
- смена пароля должна происходить каждые 90 дней;
- минимальная длина пароля должна составлять не менее 7 символов;
- пароль должен содержать как цифры, так и буквы разного регистра;
- не использовать 4 ранее используемых пароля;
- производить блокировку учетной записи после 6 неудачных попыток входа минимум на 30 минут (или до разблокировки администратором).

Также пользователи должны выполнять следующие действия по обеспечению безопасного доступа:

- изменять пользовательские пароли, по крайней мере, каждые 90 дней;
- при отсутствии активности во время пользовательского сеанса более чем 15 минут необходимо обеспечить выполнение повторного запроса пароля пользователя для разблокировки терминала.

Доступ к ПК, серверам и базам данных платежного приложения необходимо осуществлять в соответствии с требованиями п. 3.1—3.2 стандарта PA-DSS (указанным в текущем документе в разделе «10. Настройка доступа»).

11. ЖУРНАЛЫ АУДИТА

На ПК УС должен быть установлен инсталлятор политики безопасности ОС Windows «TellME Advanced Security» или произведены ручные настройки в соответствии с требованиями стандарта PA-DSS, указанными в текущем разделе.

Внимание!

Запрещается отключать ведение журналов аудита после установки инсталлятора политики безопасности ОС Windows, так как это может привести к несоответствию требованиям стандарта PA-DSS.

С помощью инсталлятора политики безопасности ОС Windows «TellME Advanced Security» реализуется автоматическое ведение журналов аудита отслеживания и контроля доступа пользователей к сетевым ресурсам и данным платежных карт.

После установки политики безопасности «TellME Advanced Security» клиентам необходимо дополнительно отключить возможность использования точек восстановления ОС Windows. Для этого поставьте галочку «Turn off System Restore on all drives», расположенную в настройках Windows «Start» => «Control Panel» => «System» => «System properties» => «System Restore».

Инсталлятор политики безопасности дополнительно включает аудит на доступ к файлам, содержащим критичные данные (представленные в настоящем документе в разделе «8.1. Хранение данных платежных карт в журналах»), аудит на ключи реестра. При настройках политики безопасности самостоятельно необходимо включить аудит вручную (подробнее см. (см. документ «Утилита “TellME Advanced Security”. Руководство по установке и настройке», раздел «Настройка политики безопасности ОС самостоятельно»).

11.1. Резервное копирование журналов аудита

Клиентами и дилерами/системными интеграторами должно оперативно выполняться резервное копирование журналов аудита на централизованный сервер протоколирования или на отдельный носитель, где их изменение было бы затруднено. Особенно важно производить копирование журналов Security Event Log.

Журналы ОС **Windows 10** по умолчанию хранятся в папках:

- Журнал «Безопасности» — %SystemRoot%\System32\Winevt\Logs\Security.evtx.
- Журнал «Приложений» — %SystemRoot%\System32\Winevt\Logs\Application.evtx.
- Журнал «Системы» — %SystemRoot%\System32\Winevt\Logs\System.evtx.

Журналы ОС **Windows 7** по умолчанию хранятся в папках:

- Журнал «Безопасности» — %SystemRoot%\System32\Winevt\Logs\Security.evtx.
- Журнал «Приложений» — %SystemRoot%\System32\Winevt\Logs\Application.evtx.
- Журнал «Системы» — %SystemRoot%\System32\Winevt\Logs\System.evtx.

Журналы ОС **Windows XP** по умолчанию хранятся в папках:

- Журнал «Безопасности» — %SystemRoot%\System32\config\SecEvent.Evt.
- Журнал «Приложений» — %SystemRoot%\System32\config\AppEvent.Evt.
- Журнал «Системы» — %SystemRoot%\System32\config\SysEvent.Evt.

Кроме того рекомендуется использовать продукт для управления ИТ-инфраструктурой на основе Microsoft Windows и смежных устройств «Microsoft System Center Configuration Manager (SCCM)».

12. ИСПОЛЬЗОВАНИЕ ПРОТОКОЛОВ И СЕРВИСОВ

Для устранения новых проблем, связанных с уязвимостями, при использовании ПО «TellME 7» должны быть отключены все ненужные и небезопасные сервисы и протоколы (сервисы и протоколы, не являющиеся необходимыми для выполнения назначенных устройствам функций).

Установка основных настроек политики безопасности производится инсталлятором политики безопасности «TellME Advanced Security» (см. документ «Утилита “TellME Advanced Security”. Руководство по инсталляции и настройке», раздел «Инсталляция утилиты “TellME Advanced Security”»).

Правила работы служб для соответствия требованиям PA-DSS, указанным в текущем разделе настоящего документа, можно также настроить вручную.

Для передачи данных платежного приложения клиентам рекомендуется использовать протокол TCP/IP. ПО «TellME 7» не требует предопределенных IP-портов. Настройки соединения производятся клиентскими организациями самостоятельно.

13. ИСПОЛЬЗОВАНИЕ БЕСПРОВОДНЫХ ТЕХНОЛОГИЙ

ПО «TellME 7» не требует использования беспроводных технологий. При использовании клиентами и дилерами/системными интеграторами беспроводных технологий необходимо установить межсетевой экран (МЭ) и обеспечить надежную защиту передаваемой информации. В соответствии с требованиями *стандарта PCI DSS* МЭ должны быть установлены для организации защиты периметра между любыми беспроводными сетями и средой платежных карт. Конфигурация межсетевых экранов должна обеспечивать блокирование любого трафика из беспроводных сетей в среду данных платежных карт или контроль этого трафика (если такой трафик необходим для ведения бизнеса).

Перед внедрением беспроводных технологий организация должна соотнести необходимость их использования с риском от их применения.

Для соответствия с требованиями *стандарта PCI DSS* в беспроводных сетях, подключенных к среде данных платежных карт или в которых передаются данные платежных карт, должны быть изменены значения, заданные производителем по умолчанию, включая (но не ограничиваясь) следующие параметры: ключи шифрования в беспроводных сетях, пароли и SNMP-строки. Убедитесь, что заданы параметры безопасности для технологии надежного шифрования, используемые для авторизации пользователей и передачи данных.

В соответствии с требованиями **стандарта PCI DSS** в беспроводных сетях, в которых передаются данные платежных карт или подключенных к среде данных платежных карт, для реализации надежного шифрования при авторизации и передаче данных должен использоваться накопленный в отрасли опыт (например, стандарт IEEE 802.11i).

- Запрет использования протокола WEP.
- Смена значений, установленных производителем по умолчанию.
- Отключение трансляции SSID сети.
- Установка MAC, IP фильтрации.
- Использование WPA2 протокола с минимальной длиной ключа 128 бит и 24 вектор инициализации.
- Запрет доступа к настройкам точки доступа или роутера через беспроводную сеть.
- Физическая защита точек доступа.

14. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ СРЕДЫ ЭКСПЛУАТАЦИИ

ПО «TellME 7» не требует, чтобы сервер базы данных и WEB-сервер находились на одном сервере или в одной DMZ.

Внимание!

Для соответствия требованиям **PA-DSS** клиентам или дилерам/системным интеграторам запрещено хранение данных платежных карт в системах, доступных из сети Интернет (WEB-сервер и сервер базы данных не должны находиться на одном сервере).

15. УДАЛЕННЫЙ ДОСТУП

Средствами ПО «TellME 7» не предоставляется возможность удаленного доступа к ПК УС.

Если у дилеров/системных интеграторов или клиентов возникает необходимость использовать удаленный доступ к ПК УС, на котором установлено ПО «TellME 7», то удаленный доступ должен быть реализован безопасными методами и аутентифицирован с помощью механизма двухфакторной аутентификации. При прохождении аутентификации необходимы как пароль, так и дополнительный элемент аутентификации (смарт-карта, PIN к аппаратному устройству аутентификации). Должны использоваться такие технологии, как RADIUS или TACACS с аппаратными устройствами аутентификации; либо VPN (на базе протоколов SSL/TLS или IPSEC) с пользовательскими сертификатами.

Для защиты удаленного доступа необходимо соблюдать требования **стандарта PCI DSS**:

- 1) Каждому пользователю должен быть присвоен уникальный идентификатор до предоставления доступа к системным компонентам или данным платежных карт.
- 2) В дополнение к назначению уникального идентификатора для всех пользователей должен использоваться по крайней мере один из следующих механизмов аутентификации:
 - пароль или кодовая фраза;

- двухфакторная аутентификация (например, устройства аутентификации, смарт-карты, биометрия или открытые ключи).
- 3) Для предоставления удаленного доступа (доступа сетевого уровня, осуществляемого из-за пределов внутренней сети) в сеть служащим компании, администраторам или третьим лицам должна быть реализована двухфакторная аутентификация. Должны использоваться такие технологии, как RADIUS или TACACS с аппаратными устройствами аутентификации; либо VPN (на базе протокола TLS 1.2 или IPSEC) с пользовательскими сертификатами.
- 4) Все пароли должны быть приведены к нечитаемому виду при передаче и хранении на всех системных компонентах с помощью алгоритмов надежной криптографии (определение термина «надежная криптография» см. в разделе «Список терминов и сокращений» настоящего документа).
- 5) Для учетных записей сотрудников и администраторов на всех системных компонентах должны обеспечиваться надежная аутентификация и управление паролями, как описано в нижеследующих пунктах:
- должно контролироваться добавление, удаление и изменение пользовательских идентификаторов, учетных данных и других объектов идентификации;
 - должна выполняться проверка подлинности пользователей перед сбросом их паролей;
 - первоначальные пароли для каждого пользователя должны быть уникальными и изменяться сразу же после первого использования;
 - доступ для каждого сотрудника при его увольнении должен немедленно аннулироваться;
 - должно выполняться удаление/отключение неактивных учетных записей пользователей по крайней мере каждые 90 дней;
 - учетные записи, используемые производителями для осуществления удаленной поддержки, должны активироваться только на период оказания поддержки;
 - парольные политики и процедуры должны быть доведены до всех пользователей, обладающих возможностью доступа к данным платежных карт;
 - не должны использоваться групповые, разделяемые или встроенные учетные записи и пароли;
 - пользовательские пароли должны меняться по крайней мере каждые 90 дней;
 - длина паролей должна составлять не менее 7 символов;
 - пароли должны содержать как цифры, так и буквы;
 - должно быть запрещено задание нового пароля, если он совпадает с любым из последних четырех ранее использовавшихся паролей;
 - количество неудачных попыток получения доступа должно быть ограничено блокированием идентификатора пользователя по крайней мере после 6 неудачных попыток;
 - продолжительность блокирования идентификатора пользователя должна составлять минимум 30 минут или до активации учетной записи администратором;

- при отсутствии активности во время пользовательского сеанса более чем на 15 минут должен выполняться повторный запрос пароля пользователя для разблокирования терминала.

16. ПЕРЕДАЧА ДАННЫХ ПЛАТЕЖНЫХ КАРТ ПО СЕТЯМ ОБЩЕГО ПОЛЬЗОВАНИЯ

Для надежной защиты передаваемых критических данных платежных карт ПО «TellME 7» необходимо использовать технологии VPN или другие надежные методы обеспечения безопасности устройств самообслуживания.

Если клиентам или дилерам/системным интеграторам необходимо передавать данные платежных карт по сетям общего пользования, то в соответствии с требованиями PCI DSS должны использоваться методы надежной криптографии и протоколы шифрования (в соответствии с требованиями стандарта PCI DSS), обеспечивающие защиту критичных данных платежных карт, передаваемых по открытым сетям общего пользования.

ПО «TellME 7» не передает номера PAN с помощью технологий обмена сообщениями между конечными пользователями.

17. НЕКОНСОЛЬНЫЙ АДМИНИСТРАТИВНЫЙ ДОСТУП

Клиентам или дилерам/системным интеграторам необходимо в обязательном порядке шифровать каждый неконсольный административный доступ, используя безопасные технологии (такие как TLS 1.2, VPN), для управления с помощью WEB-интерфейса и других типов неконсольного административного доступа.

Использование открытых протоколов Telnet и rlogin для административного доступа запрещается.

18. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ ОТЛАДКИ В ТЕСТОВОМ РЕЖИМЕ

18.1. Формирование данных RMS-журнала

В RMS-журнале трассируется трафик обмена данными в канале в неизменном виде.

Для включения/выключения формирования журнала RMS в тестовом режиме (тестовый режим должен быть прописан на ключе лицензионной защиты) необходимо в ветке реестра [HKEY_CLASSES_ROOT\WOSA\XFS_ROOT\ATM\PaymentSystems\<Наименование платежной системы>\Config\Channel] присвоить параметру «LogTraffic» следующие значения:

«LogTraffic»=dword:00000000 — отключено формирование журнала RMS;

«LogTraffic»=dword:00000001 — включено формирование журнала RMS (возможно только в тестовом режиме).

При вставлении пользовательской карты в ридер на экран выдается предупреждение о работе УС в тестовом режиме. В тестовом режиме в RMS-журналы прописываются данные, передаваемые по каналу связи с процессинговым центром.

Файл журнала в тестовом режиме сохраняется как C:\SCS\LOGS*Наименование платежной системы*\RMS\YYYYMMDD.RMS.

18.2. Конфигурация для приема карт стандарта «EMV»

Значения нижеприведенных секций устанавливаются по умолчанию. Значения параметров для приема карт стандарта «EMV» можно изменить только в тестовом режиме использования УС (тестовый режим должен быть прописан на ключе лицензионной защиты). При использовании тестового ключа автоматически включается режим расширенной трассировки данных EMV CORE.

Конфигурирование «EMV» можно выполнить (в тестовом режиме) в файле C:\SCS\ATM_H\DataNDC\emv_ndc.cfg или C:\SCS\ATM_H\DataNDC2\emv_ndc.cfg.

Секция [Trace] — данная секция задает режим журнализации ПМ «EMV CORE»™. Секция может содержать следующие параметры:

- TraceLevel — режим хранения журналов, где
 - 0 — не сохранять журналы (по умолчанию);
 - 1 — сохранять журналы, если транзакция завершилась неуспешно;
 - 2 — всегда сохранять журналы.
- FileHistory — период хранения EMV-журналов, в днях (по умолчанию 90 дней);
- Path — абсолютный или относительный путь к каталогу (C:\SCS\ATM_H), в котором следует сохранять журналы. По умолчанию журналы сохраняются в каталоге C:\SCS\LOGS\NDC\EMV или C:\SCS\LOGS\NDC2\EMV.
- MinFileCount = 10 — количество журналов, не подлежащих удалению (10 последних файлов).

Внимание!

При работе ПО «TellME 7» в тестовом режиме для проведения тестовых платежных операций должны использоваться только тестовые карты. **Запрещается** повторное использование карт реальных клиентов с истекшим сроком действия!

19. ПО СТОРОННИХ ПРОИЗВОДИТЕЛЕЙ

ПО «TellME 7» предназначено для работы на стандартном PC-совместимом компьютере, с предустановленными Windows XP (Windows Embedded POSReady 2009), Windows 7 (Windows Embedded POSReady 7) и ОС Windows 10 (Windows 10 IoT Enterprise LTSC 2016 (v.1607), Windows 10 IoT Enterprise LTSC 2019 (v.1809)). Каждый производитель УС представляет свой тип и конфигурацию ОС, которую необходимо устанавливать на УС.

На банкоматах «NCR» ПО «TellME 7» работает с ПО производителя «Aptra XFS».

На банкоматах «Wincor Nixdorf» ПО «TellME 7» работает с ПО производителя «CSC-W32» или «ProBase».

На банкоматах «Diebold Nixdorf» ПО «TellME 7» работает с ПО производителя «ProBase».

На банкоматах «Diebold» ПО «TellME 7» работает с ПО производителя «Agilis XFS».

На банкоматах «Nautilus Hyosung» ПО «TellME 7» работает с ПО производителя «Nextware».

На банкоматах «OKI» ПО «TellME 7» работает с ПО производителя «OKI-SP».

На банкоматах «GRG» ПО TellME 7» работает с ПО производителя «GRG XFS».

20. ВЕРСИИ И МОДИФИКАЦИИ

В процессе разработки в согласованные моменты времени в соответствии с календарным планом разработки производится сборка готовой версии проекта. Готовому для сборки проекту присваивается уникальный номер версии и номер сборки. Нумерация версий и сборок начинается от нуля.

Присвоение номера версии и проставление метки (label) на соответствующий проект конфигурационного управления производится специально выделенным специалистом.

По окончании сборки производится тестирование ПО.

Нумерация версий и сборок

Типы изменений	Критерии	Примеры	Изменения версии
High-impact	<p>Изменения в ПО удовлетворяют <i>любому</i> из условий:</p> <ul style="list-style-type: none"> • 4 или больше разделов (с 1 по 12) стандарта затронуто; • больше половины всех требований (разделов с 1 по 12) стандарта затронуто; • больше половины функционала (либо кода) ПО изменено; • дополнительные платформы/ОС необходимо добавить в перечень поддерживаемых 	Крупные изменения в ПО, глобальные переделки (например, при адаптации ПО на соответствие стандарта PA-DSS)	Изменяется первая цифра (например, 1.0 на 2.0)

Типы изменений	Критерии	Примеры	Изменения версии
Low-impact	<p>Изменения в ПО удовлетворяют <i>всем</i> условиям:</p> <ul style="list-style-type: none"> • меньше 4-х разделов (с 1 по 12) стандарта затронуто; • меньше половины всех требований стандарта (разделов с 1 по 12) затронуто; • меньше половины функционала (либо кода) ПО изменено 	<ul style="list-style-type: none"> • изменения для работы с обновленными версиями проверенных ранее версий ОС, стороннего ПО; • добавление нового типа функциональности; • перекомпиляция исходного кода с использованием нового компилятора/новых настроек компилятора; • изменение политики версионности ПО; • обновления ПО не связанные с безопасностью 	Изменяется первая или вторая цифра (например, 1.0 на 1.1)
No impact	<p>Изменения ПО не влияющие на его безопасность и не влияющие на выполнение требований PA-DSS</p>	<p>Модификация существующей функциональности:</p> <ul style="list-style-type: none"> • изменения в пользовательском интерфейсе; • изменения алгоритма обработки чтения пластиковой карты 	Изменяется инкрементируемая часть, не влияющая на сертификацию (например, 1.0.5 на 1.0.6 (при сертификации 1.0.x))

Типы изменений	Критерии	Примеры	Изменения версии
Administrative	Изменения не связанные с разработкой ПО	<ul style="list-style-type: none">• изменение наименования ПО;• изменение наименования вендора	Версия ПО не меняется

21. ИСТОРИЯ ИЗМЕНЕНИЙ ДОКУМЕНТА

Дата изменений	Версия док-та	Описание изменений
18.08.2021	01.00	Исходная редакция документа, разработанная с учетом требований PCI DSS (версия 3.2) и PA-DSS (версия 3.2)