



SmartCard-Service

Акционерное общество «СмартКард-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

У Т В Е Р Ж Д Е Н О

Генеральный директор

АО «СмартКард-Сервис»

\_\_\_\_\_ В.А. Васильев

№ \_\_\_\_\_ «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г.

## Программа «Удостоверяющий центр CA.RUS»

### УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ (VULNERABILITY MANAGEMENT)

Файл: управление уязвимостями.doc

Москва  
2024

## СОДЕРЖАНИЕ

1. Сведения о документе .....	3
2. Введение.....	4
3. Список терминов и сокращений.....	5
4. Идентификация уязвимостей в разрабатываемом ПО .....	6
5. Идентификация уязвимостей ПО сторонних производителей.....	7
6. Меры обеспечения информационной безопасности ПК УС.....	10
7. История изменений документа .....	11

## 1. СВЕДЕНИЯ О ДОКУМЕНТЕ

Номер версии:	01.02
Дата выпуска:	19.10.2023 г.
Дата утверждения:	
Частота пересмотра:	1 раз в год

## 2. ВВЕДЕНИЕ

Настоящий документ является частью организационного обеспечения разработки программного обеспечения сотрудниками АО «СмартКард-Сервис». В документе «Управление уязвимостями» (далее - Документ) содержится описание процедур обеспечения информационной безопасности разработки программного обеспечения (ПО). Для обеспечения соответствия стандарту PCI SSF. Документ регламентирует действия со стороны производителя, направленные на своевременную идентификацию уязвимостей и возможные пути их разрешения. На основе данного Документа разрешаются требования стандарта PCI SSF.

При разработке ПО для идентификации потенциальных уязвимостей сотрудниками АО «СмартКард-Сервис» производятся регулярные проверки внешних уязвимостей.

Документ содержит 11 страниц.

### 3. СПИСОК ТЕРМИНОВ И СОКРАЩЕНИЙ

Сокращение	Расшифровка сокращения
PCI SSF	Семейство стандартов, направленных на обеспечение безопасности программного обеспечения (PCI Software Security Framework), на данный момент состоит из двух связанных между собой стандартов — Secure Software Standard (SSS) и Secure Software Lifecycle (Secure SLC) Standard
PCI SSS	Стандарт безопасности данных программного обеспечения индустрии платежных карт (Payment Card Industry Security Software Standard)
PCI SLC	Стандарт, который определяет безопасные методы управления жизненным циклом платёжного ПО, позволяющие гарантировать производителю такого ПО, что оно спроектировано и разработано для защиты платежных транзакций и данных, минимизации уязвимостей, и защиты от атак
ПО	Программное обеспечение
Программа «Удостоверяющий центр CA.RUS»	Программа реализует функционирование Удостоверяющего Центра для выполнения цифровой подписи публичных ключей EPP-клавиатур и Хоста.
УС	Устройство самообслуживания

## 4. ИДЕНТИФИКАЦИЯ УЯЗВИМОСТЕЙ В РАЗРАБАТЫВАЕМОМ ПО

Все выявленные уязвимости фиксируются в отдельном журнале, включающем в себя: наименование уязвимости, ее применимость для разрабатываемого ПО, методы устранения уязвимости, отметку о факте тестирования и его работоспособности при обновлении компонентов инфраструктуры ПО, дату обнаружения и тестирования, ФИО сотрудника, степень критичности на основании CVSS 3.1.

Все выявленные уязвимости должны быть оценены по степени критичности на основании значений CVSS 3.1. Уязвимости со значением CVSS 3.1 больше или равной 4 должны быть отмечены как критичные, и устранены в течение 5 рабочих дней. При необходимости в ПО должны быть внесены необходимые изменения с целью минимизации влияния выявленных уязвимостей. Уязвимости со значением CVSS 3.1 меньше 4 должны быть устранены не более, чем через 10 рабочих дней после их обнаружения.

При получении от клиента информации об обнаружении в разрабатываемом ПО угроз данным платежных карт и недостатков снижающих общий уровень безопасности приложения, необходимо в течение двух рабочих дней определить характер недостатка и степень критичности соответствующей уязвимости. Устранение уязвимости должно осуществляться в срок, соответствующий определенной степени критичности.

На время устранения любых обнаруженных уязвимостей, необходимо разработать, и передать клиентам временное решение обеспечивающее снижение рисков от возможной реализации выявленных уязвимостей.

## 5. ИДЕНТИФИКАЦИЯ УЯЗВИМОСТЕЙ ПО СТОРОННИХ ПРОИЗВОДИТЕЛЕЙ

Для своевременной идентификации уязвимостей ПО сторонних производителей организован процесс обнаружения уязвимостей безопасности (Рис. 1).

Специалисты Группы Контроля Качества на периодической основе (приблизительно один раз в неделю) исследуют на появление новых уязвимостей. Анализ влияния обнаруженных уязвимостей на ПО и необходимость дополнительного тестирования и внесения изменений производится в соответствии с представленной ниже диаграммой (см. Рис. 1). На периодической основе при возникновении уязвимостей безопасности, имеющих возможность идентификации в ПО, производится информирование группы разработчиков с обсуждением возможностей предотвращения уязвимостей. В процессе анализа производится ранжирование уязвимостей в диапазоне от 1 до 4.

К уровню 1 относятся уязвимости, обнаруженные в программах, WEB-сервисах, библиотеках сторонних производителей, которые не устанавливаются, не могут быть установлены на УС и эксплуатироваться вместе с ПО. Такие уязвимости не являются критичными и не будут влиять на качество выпускаемого ПО. Дальнейшее тестирование не требуется.

К уровню 2 относятся уязвимости, обнаруженные в программах, WEB-сервисах, библиотеках сторонних производителей, которые не рекомендуются для использования или не используются совместно с ПО, но могут быть установлены клиентами и дилерами/системными интеграторами самостоятельно. Безопасность работы с этими программами, WEB-сервисами или библиотекам обеспечивают клиенты и дилеры/системные интеграторы самостоятельно. Уязвимости такого типа имеют «Низкий» уровень критичности. Тестирование совместно с ПО проводится на стороне клиентов и дилеров/системных интеграторов.

К уровню 3 относятся уязвимости, обнаруженные в блоках среды эксплуатации, в программах, библиотеках сторонних производителей аппаратных модулей, которые могут быть установлены на УС, но не взаимодействуют с ПО. Таким уязвимостям присваивается «Средний» уровень критичности.

К уровню 4 относятся уязвимости, обнаруженные в программах, WEB-сервисах, библиотеках сторонних производителей, которые устанавливаются или имеют доступ к УС с установленным ПО или с которыми ПО взаимодействует непосредственно в процессе работы. Таким уязвимостям присваивается «Высокий» уровень критичности.

Для уязвимостей 3 и 4 уровня требуется дополнительный анализ влияния на работу ПО. При необходимости, на основе данной уязвимости в специализированном средстве управления запросами на изменение программного продукта «Rational ClearQuest» создается заявка типа «Feature Request» или «Defect Request», на основании которой вносятся изменения в код программы и/или требуется дополнительное тестирование.

Процесс обработки заявок по уязвимостям ПО сторонних производителей аналогичен жизненному циклу обработки заявок, представленному в документе «Организация и процессы сопровождения ПО».

Если обнаруженные уязвимости являются критичными в работе ПО, то принимается решение о выпуске новой версии ПО или соответствующего обновления/дополнения к

текущей версии. На представленной далее диаграмме отображен процесс анализа влияния уязвимостей и дальнейший процесс их обработки.

Сотрудники АО «СмартКард-Сервис» информируются производителями УС об идентификации новых уязвимостей и внесении соответствующих изменений в аппаратные модули устройств и в платформы взаимодействия с устройствами. Все изменения в программно-аппаратный комплекс производителей УС и новые версии программно-аппаратных комплексов проходят обязательное тестирование совместно с ПО.

Тестирование осуществляется в соответствии с документом «Положение о тестировании в проектах разработки ПО», входящем в состав документации по процессам производства программного обеспечения в АО «СмартКард-Сервис».

Сотрудники АО «СмартКард-Сервис» на периодической основе исследуют сайты компании «Microsoft» на появление новых уязвимостей, таким образом, сотрудники своевременно информируются об изменениях, связанных с информационной безопасностью и обнаружением уязвимостей в продуктах компании «Microsoft», которые необходимы для работы ПО, включая обновления ОС. Необходимые исправления можно получить из рассылки или скачать свободно доступные обновления из сети Интернет.



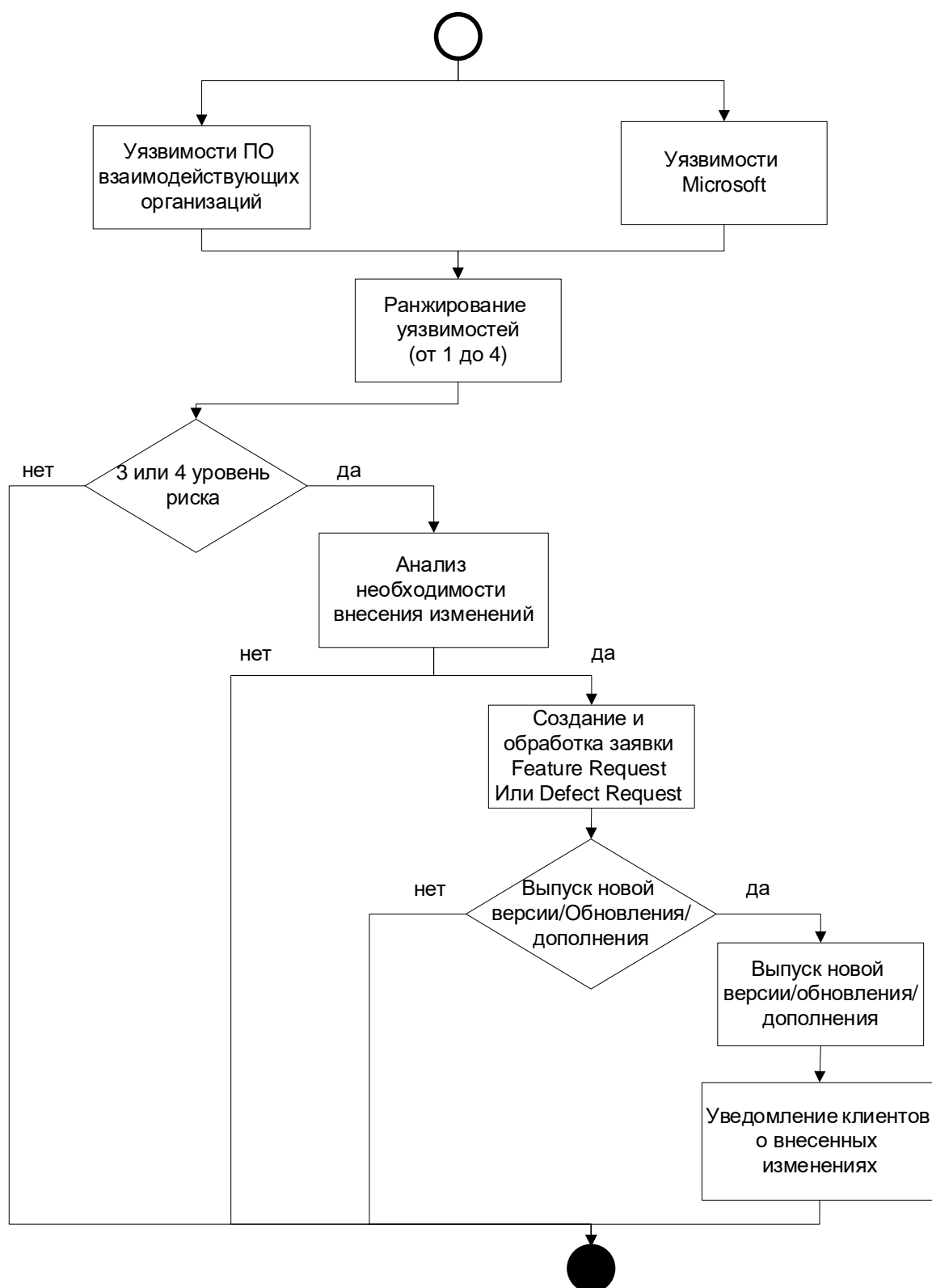


Рис. 1. Процесс идентификации новых уязвимостей и анализ их влияния

## 6. МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПК УС

Если результаты тестирования показали корректную работу ПО с обновлениями или изменениями ПО сторонних производителей, связанными с информационной безопасностью, то клиентам или дилерам/системным интеграторам рекомендуются к использованию данные обновления или изменения.

При выполнении тестирования обновлений и изменений могут потребоваться дополнительные доработки ПО для корректного взаимодействия с выпущенными обновлениями или изменениями ПО сторонних производителей. Архитектор проекта устанавливает сроки внесения необходимых изменений в ПО.

**Примечание.** Архитектор проекта — лицо, ответственное за ежедневное управление проектом, командой проекта. Он также несет ответственность за полноту и целостность состояния разрабатываемого проекта в целом.

По результатам работ выпускается обновление или новые версии ПО, поддерживающие работу с обновлениями или изменениями ПО сторонних производителей. Правила выпуска версий и обновлений ПО зафиксированы в документе «План конфигурационного управления», входящем в состав документации по процессам производства ПО в АО «СмартКард-Сервис». Клиентам или дилерам/системным интеграторам рекомендуются к использованию выпущенные версии и обновления ПО.

Удаленный доступ к ПК УС, инсталляция обновлений ПО и ПО сторонних производителей осуществляется клиентами или дилерами/системными интеграторами самостоятельно.

## 7. ИСТОРИЯ ИЗМЕНЕНИЙ ДОКУМЕНТА

Дата изменений	Версия док-та	Описание изменений
17.08.2022	01.00	Исходная редакция документа, разработанная с учетом требований PCI DSS (версия 3.2.1) и PA-DSS (версия 3.2)
25.08.2022	01.01	Внесены корректировки, учитывающие требования PCI DSS (версия 4.0), PCI SLC v.1.1 и PCI SSS v.1.1
19.10.2023	01.02	Документ пересмотрен с учетом изменений в стандарте PCI SSS v.1.2.1