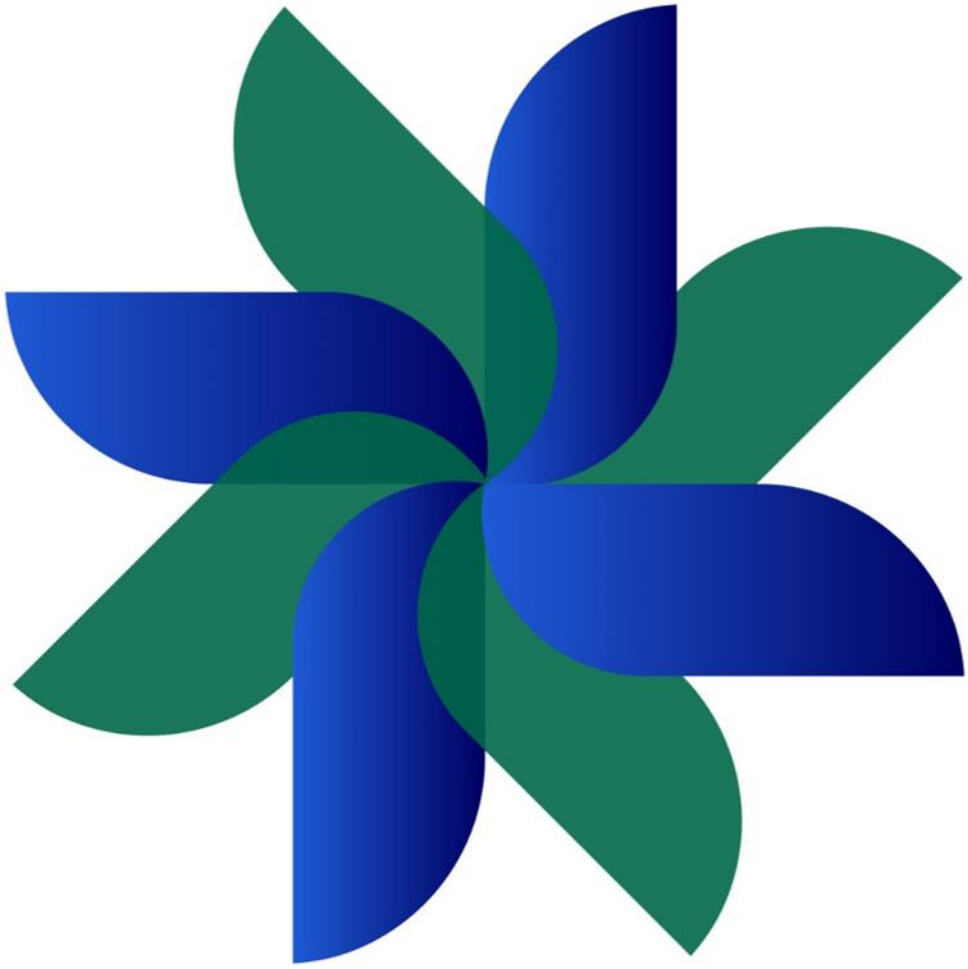
Стандарт ПС «Мир».
Обеспечение безопасности при использовании Карт в Нефинансовых сервисах

П.258

Версия 2.0



НСПК
Москва, 2024

Оглавление

1. Общие положения

1.1. Назначение и область применения документа

Настоящий документ устанавливает требования и рекомендации для организаций, которые разрабатывают, внедряют и эксплуатируют системы, использующие Карты в целях, не связанных с осуществлением Финансовых операций (то есть в Нефинансовых сервисах), и организаций, которые обрабатывают данные Карт вне рамок осуществления Финансовых операций. Примерами такого использования являются:

- использование полного номера Карты как идентификатора проездного билета для оплаты проезда на общественном транспорте, а также использование Карт для реализации права льготного проезда на общественном транспорте и для реализации функционала «стоп-листов» в автоматизированных системах оплаты проезда, в которых для оплаты проезда принимаются Карты;
- использование Карт в качестве пропуска на территорию организации или в помещения зданий;
- использование Карт как единого идентификатора в СКУД и платежно-пропускных системах, в том числе в образовательных организациях, – доступ в помещения, «электронная» зачетная книжка, «электронный» билет в библиотеку, «электронное» служебное удостоверение, «электронный ски-пасс» и т.п.;
- использование Карт как идентификатора в многофункциональных центрах предоставления государственных и муниципальных услуг (МФЦ, «Мои документы»), органах социальной защиты, медицинских организациях или иных государственных организациях для ускоренного обслуживания в системах электронных очередей и на рабочем месте оператора (сотрудника) при приеме заявления на оказание услуги или выдаче результата оказания услуги;
- использование Карт в системе социального обслуживания и здравоохранения как инструмента идентификации льготника, а также инструмента предоставления мер социальной поддержки в виде денежных выплат или в натуральной форме, в том числе идентификатора в системе лекарственного обеспечения;
- использование Карт в качестве идентификаторов в различных программах лояльности, операторами (организаторами) которых выступают органы государственной власти, органы местного самоуправления, государственные или коммерческие организации и др.

1.2. Термины, определения и сокращения

CMAC – Cipher-based Message Authentication Code, имитовставка на основе блочного алгоритма шифрования.

HMAC – Keyed-hash Message Authentication Code, имитовставка на основе функций хеширования с секретным ключом.

HSM – Hardware Security Module.

SAM – Security Access Module.

БД – база данных.

Данные Карты – набор данных, включающий данные о держателе карты и критичные аутентификационные данные, указанные в документе «PCI DSS and PA-DSS. Glossary of Terms, Abbreviations, and Acronyms»[1].

Держатель Карты – физическое лицо, в качестве Клиента использующее Карту на основании договора с Эмитентом, или физическое лицо, являющееся уполномоченным представителем Клиента.

Кампусный проект – Нефинансовый сервис, в котором осуществляется считывание и обработка данных Карт в устройствах, не предназначенных для обработки финансовой информации и формирования авторизационных запросов, например, в рамках контрольно-пропускных систем и СКУД.

Карта – электронное средство платежа, в том числе эмитированная Участником платежная Карта или ее реквизиты, являющееся средством для составления расчетных и иных документов, подлежащих оплате за счет Клиента.

Критичные аутентификационные данные – реквизиты Карты ПС «Мир», включающие в себя следующие данные:

- ППК2;
- полное содержимое дорожек магнитной полосы Карты, эквивалентные им данные с чипа, а также содержимое дорожек магнитной полосы Карты слева от сервисного кода;
- ПИН-код и ПИН-блок.

[1] Документ *«PCI DSS and PA-DSS. Glossary of Terms, Abbreviations, and Acronyms»* на русском и английском языке доступен на сайте https://www.pcisecuritystandards.org/document_library.

Нефинансовый сервис – сервис, в котором используются Карты в целях, не связанных с осуществлением Финансовых операций.

ОС – операционная система.

СКЗИ – средства криптографической защиты информации.

СКУД – система контроля и учета доступа.

Считыватель Карт – специализированное устройство, выполняющее считывание реквизитов Карты для криптографического преобразования номера Карты посредством хеширования или шифрования и дальнейшего использования полученного значения для идентификации Держателя Карты в рамках Нефинансового сервиса.

УЗ – учетная запись.

Финансовая операция – перевод денежных средств с использованием Карты (реквизитов Карты).

Термины и определения, не раскрытые в настоящем документе, используются в значении терминов и определений, приведенных в Правилах ПС «Мир».

1.3. Ответственность за соблюдение требований

1.3.1. Положения данного Стандарта, содержащие слова «необходимо», «должно/должны», «запрещено», являются обязательными к исполнению.

1.3.2. Положения данного Стандарта, содержащие слово «рекомендуется», не являются обязательными к исполнению. При этом невыполнение рекомендаций возможно только при наличии веских причин, которые препятствуют их выполнению (например, обоснованные технологические ограничения).

1.3.3. Участник несет ответственность перед АО «НСПК» за соблюдение данного Стандарта организациями, которые предоставляют Нефинансовые сервисы на основании договорных отношений с Участником, организациями, которые на основании договорных отношений с Участником выполняют разработку, внедрение и/или эксплуатацию систем, используемых для предоставления Нефинансовых сервисов, а также организациями, которые на основании договорных отношений с Участником обрабатывают данные Карт вне рамок осуществления Финансовых операций.

1.3.4. АО «НСПК» оставляет за собой право запрашивать дополнительные сведения и документы, подтверждающие выполнение положений Стандарта. По запросу АО «НСПК» Участник должен представить запрошенную информацию или документы в порядке и сроки, указанные в запросе АО «НСПК».

1.4. Нормативные ссылки

[1] *Правила Платежной системы «Мир».*

[2] *Стандарт ПС «Мир». Программа безопасности.*

[3] *Операционный бюллетень #45.2019 от 23.10.2019. Персонализация нефинансового экземпляра платежного приложения «Мир».*

1.5. Уведомления

Перевод документов

Перевод любого документа, разработанного АО «НСПК», может быть выполнен третьим лицом исключительно после получения письменного разрешения АО «НСПК». АО «НСПК» не контролирует и не несет ответственности за содержание переведенного текста документа.

Переведенные тексты документов, разработанных АО «НСПК», применяются третьим лицом исключительно в целях установления содержания и смысла этих документов и не имеют юридической силы.

Тексты документов, составленных на русском языке, имеют приоритет перед текстами на другом языке.

2. Общие требования к использованию реквизитов Карт в Нефинансовых сервисах

2.1 В рамках Нефинансовых сервисов допускается обработка только следующих данных, являющихся данными (реквизитами) Карты: номер Карты, имя и фамилия Держателя Карты. Запрещается обработка других данных (реквизитов) Карт, в том числе срока действия Карты, сервисного кода, Критичных аутентификационных данных[2].

2.2 В рамках Нефинансовых сервисов запрещено использование полного номера Карты в открытом виде в целях идентификации Держателя Карты.

2.3 Для идентификации Держателя Карты в рамках Нефинансовых сервисов с помощью Карты необходимо использовать значение, полученное после криптографического преобразования полного номера Карты посредством хеширования или шифрования.

2.4 Данные Карт, сохраняемые в рамках процесса хеширования или шифрования, должны храниться в системе или устройстве, выполняющем преобразование, в течение периода времени, минимально необходимого для преобразования номера Карты, после чего должны надежно удаляться из памяти системы или устройства.

2.5 Преобразование полного номера Карты в хешированное или шифрованное значение должно выполняться на устройстве, которое выполняет считывание реквизитов Карты (POS-терминале, валидаторе, Считывателе карт, и т.д.). Если преобразование выполняется не на считывающем устройстве, а на стороне серверной части Нефинансового сервиса, то должна обеспечиваться конфиденциальность полного номера Карты при его передаче между компонентами такого сервиса.

2.6 Для обеспечения конфиденциальности данных Карт при передаче должны использоваться стойкие протоколы и алгоритмы, не содержащие известных уязвимостей. При этом минимально необходимо использование протокола TLS версии 1.2. При реализации протокола TLS должны использоваться доверенные сертификаты, при этом при использовании самоподписанных сертификатов должна использоваться привязка сертификатов или ключей (key или certificate pinning).

2.7 Для считывания реквизитов Карт рекомендуется использовать устройства, прошедшие оценку соответствия требованиям стандарта PCI PTS POI[3].

---

[2] За исключением обработки данных с чипа, эквивалентных содержимому магнитной полосы, в устройствах, выполняющих считывание реквизитов Карты.

[3] Перечень сертифицированного оборудования доступен на сайте https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices.

2.8 Если для осуществления целей обработки данных и/или идентификации Держателей Карт в рамках Нефинансового сервиса могут использоваться иные данные, не являющиеся реквизитами Карт, то необходимо отказаться от использования полного номера Карты в качестве идентификатора Держателя Карты.

2.9 Организации, которые участвуют в предоставлении Нефинансовых сервисов, хранят, передают или обрабатывают данные Карт в связи с наличием обоснованной необходимости[4] их хранения, передачи или обработки в рамках Нефинансового сервиса, но при этом не задействованы в обеспечении приема Карт и (или) осуществлении Финансовых операций, должны защищать данные Карт, выполняя требования, указанные в Приложении В, или требования стандарта PCI DSS[5].

2.10 Хешированные или зашифрованные значения, полученные из полного номера Карты в полном соответствии с положениями данного Стандарта, не подлежат защите в соответствии с требованиями пункта 2.9.

2.11 Хешированные или зашифрованные значения номера Карты, которые находятся в одной инфраструктуре (локальной или распределенной вычислительной сети) с ключами их хеширования/шифрования, подлежат защите в соответствии в соответствии с требованиями пункта 2.9, если не приняты меры по изолированию хранимых хешированных/зашифрованных номеров Карт от ключей хеширования/шифрования. Возможными мерами для изолирования данных являются:

- выгрузка хешированных/зашифрованных номеров Карт или ключей хеширования/шифрования на съемные носители, доступ к которым ограничен;
- запрет логического доступа субъектам доступа (УЗ, принадлежащим одному пользователю) к ключам хеширования/шифрования одновременно с доступом к хешированным/зашифрованным с помощью указанных ключей данным. Примером реализации такого запрета является хранение хешированных/зашифрованных номеров Карт в БД и хранение ключей в файле защищенного криптографического контейнера в файловой системе, при этом пользователи с УЗ на уровне БД не должны иметь УЗ на уровне ОС, позволяющие получить доступ к ключам, включая административные УЗ, и наоборот.

4 В том числе в связи требованиями законодательства Российской Федерации.

5 Требование применимо, в том числе к системам организации, выполняющим хеширование или шифрование полного номера Карты.

2.12 Организации, которые в связи с наличием обоснованной необходимости[4] хранят, передают или обрабатывают данные Карт в целях осуществления Финансовых операций, но при этом не выполняют переводы денежных средств с использованием Карт (не осуществляют Финансовые операции), должны защищать данные Карт, выполняя требования, указанные в Приложении В, или требования стандарта PCI DSS.

2.13 Организации, которые участвуют в предоставлении Нефинансовых сервисов, хранят, передают или обрабатывают данные Карт, и задействованы в обеспечении приема Карт и (или) осуществлении Финансовых операций, должны выполнять требования стандарта PCI DSS и осуществлять подтверждение соответствия требованиям стандарта PCI DSS в соответствии с положениями подраздела 2.1 документа [2] для контура Финансовых и Нефинансовых сервисов[6].

2.14 Участник несет ответственность за обработку в соответствии с положениями документа *«Стандарт ПС “Мир”. Порядок обработки Инцидентов ИБ Участником»* инцидентов ИБ, в результате которых появились подозрения в компрометации или которые привели к компрометации данных Карт в инфраструктуре привлеченных Участником организаций, которые участвуют в предоставлении Нефинансовых сервисов и хранят, передают или обрабатывают данные Карт.

2.15 Рекомендуется исключить обработку в одной инфраструктуре усеченных и хешированных/зашифрованных версий полного номера Карты. Если обработка в одной инфраструктуре усеченных и хешированных версий полного номера Карты необходима для осуществления целей обработки данных в рамках Нефинансового сервиса, то допустимым является использование правила усечения «2 последние цифры».

[6] Требование неприменимо к организациям, которые обрабатывают зашифрованные реквизиты Карт при их передаче (например, операторы связи).

3. Использование хеширования для получения уникального идентификатора Держателя Карты

3.1 Восстановление исходного номера Карты из хешированного значения должно быть вычислительно неосуществимым.

3.2 Для хеширования полного номера Карты в Нефинансовых сервисах должны использоваться только алгоритмы HMAC с секретным ключом, реализованные на основе следующих функций хеширования: ГОСТ Р 34.11-2012, SHA-1[7], SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512), SHA-3 (SHA3-224, SHA3-256, SHA3-384, SHA3-512).

3.3 Управление ключами, используемыми при выполнении хеширования полного номера Карты, должно осуществляться в соответствии со следующими требованиями:

- должны быть разработаны и реализованы процедуры управления ключами, включая процедуры генерации, распространения и передачи, хранения, смены при подозрении на компрометацию;
- значение ключа должно уникальным для каждого типа Нефинансовых сервисов, который определяется в зависимости от используемых видов устройств считывания Карт;
- эффективная длина ключей должна составлять не менее 128 бит;
- ключи должны генерироваться с использованием специализированного криптографического оборудования (например, HSM или POS-терминалов) или с использованием надежных функций генерации псевдослучайных чисел[8];
- смена и/или уничтожение ключей, применяемых на устройствах для считывания Карт, должны производиться без необходимости вскрытия, перепрошивки или обновления устройств;
- доступ к ключу должен быть ограничен и предоставлен минимально необходимому списку лиц и/или учетных записей;
- должно быть обеспечено безопасное хранение ключей. Ключи могут храниться в специализированном криптографическом оборудовании (например, HSM, терминальных устройствах, сертифицированных по требованиям стандарта PCI PTS POI, модулях SAM, Считывателях карт,

[7] Использование HMAC на SHA1 не является рекомендуемым.

[8] Перечень рекомендуемых функций для разных языков программирования приведен в Приложении А, а также доступен на сайте OWASP в разделе Cryptographic Storage Cheat Sheet: Secure Random Number Generation.

соответствующих требованиям Приложения Б), в виде криптограммы, созданной с использованием ключа шифрования ключей не меньшей стойкости, чем защищаемый ключ, или в виде компонентов ключей при соблюдении принципов двойного контроля и разделения секрета;

- ключи шифрования ключей должны быть изолированы от защищаемых ключей хеширования с помощью мер, указанных в пункте 2.11 настоящего документа;
- должно быть обеспечено безопасное распространение и передача ключей, в том числе допустима передача ключей по защищенному каналу или передача на бумажном носителе или съемном электронном носителе, которые должны быть помещены в сейф-пакет (секьюр-пак), имеющий уникальный идентификатор;
- при передаче ключей по защищенному каналу (1) ключи должны шифроваться с использованием протокола TLS версии не ниже 1.2, (2) используемые версии шифронаборов (cipher suites) должны быть стойкими, (3) должна использоваться привязка сертификатов или ключей (key или certificate pinning), (4) должна обеспечиваться взаимная аутентификация;
- управление ключами (генерация, хранение, уничтожение, смена и т.д.) рекомендуется выполнять с использованием специализированного криптографического оборудования (например, HSM или POS-терминалов).

4. Использование шифрования для получения уникального идентификатора Держателя Карты

4.1 Для получения идентификатора из полного номера Карты с помощью функций шифрования должны использоваться стойкие алгоритмы шифрования с эффективной длиной ключа не менее 128 бит для симметричных алгоритмов, 2048 бит для асимметричных алгоритмов, 224 бит для алгоритмов на основе эллиптических кривых[9]. Допустимо использование CMAC, реализованных на основе данных алгоритмов шифрования.

4.2 При использовании асимметричных алгоритмов, включая алгоритмы на основе эллиптических кривых, для получения идентификатора из полного номера Карты, при выполнении шифрования к значению полного номера Карты путем конкатенации должно добавляться значение, которое должно соответствовать требованиям к ключам, указанными в пункте 3.3.

4.3 Управление секретными или закрытыми ключами, используемыми при выполнении шифрования полного номера Карты, должно осуществляться в соответствии требованиями, указанными в пункте 3.3.

[9] Такими алгоритмами являются: AES, ГОСТ Р 34.12-2015, RSA с ключом длины 2048 и больше, ECDSA с ключом длины 224 и больше.

5. Требования для кампусных проектов

5.1 В Кампусных проектах рекомендуется использовать Карты с установленными дополнительным приложением на базе Платежного приложения «Мир» для Нефинансовых сервисов (нефинансовым экземпляром Платежного Приложения «Мир») или Карты с установленными дополнительными приложениями на рекомендованных карточных платформах в ПС «Мир»[10].

5.2 Выпуск Карт с нефинансовым экземпляром Платежного Приложения «Мир» должен выполняться в соответствии с требованиями документа [3]. Персонализация должна проводиться со значениями PAN, Track 2 Equivalent Data, Expiration Date, Service Code, отличными от данных основного Платежного приложения. Значение Application Identifier (далее – AID) для нефинансового экземпляра Платежного приложения «Мир» должно быть согласовано с НСПК в соответствии с процедурой, установленной документом [3].

5.3 В случае использования в Кампусных проектах Карт, которые соответствуют пункту 5.1, Считыватели Карт в рамках кампусных проектов должны «запрашивать» данные исключительно от нефинансового экземпляра платежного приложения «Мир».

5.4 В случае использования в Кампусном проекте Карт, которые не соответствуют пункту 5.1 (Карт без установленного дополнительного приложения), Считыватели Карт должны соответствовать требованиям стандарта PCI PTS POI (категории устройств PED/SRED/SCRP) или требованиям к Считывателям Карт, указанным в Приложении Б.

[10] Список рекомендованных карточных платформ в ПС «Мир» доступен по ссылке https://support.nspk.ru/documents/1562.

Приложение А. Перечень функций, рекомендуемых для использования при генерации псевдослучайных величин

- для C – getrandom(2);
- для Java – java.security.SecureRandom;
- для PHP – random_bytes(), random_int(), openssl_random_pseudo_bytes();
- для NET/C# – RNGCryptoServiceProvider;
- для Objective-C – SecRandomCopyBytes;
- для Python – secrets();
- для Ruby – SecureRandom;
- для Go – crypto.rand package;
- для Rust – rand::prng::chacha::ChaChaRng, rand::prng::hc128::Hc128Rng, rand::prng::isaac::IsaacRng, rand::prng::isaac64::Isaac64Rng.

Приложение Б. Перечень требований по безопасности к Считывателям

Б.1 Механизмы физической безопасности

Б.1.1 В Считывателе должны быть реализованы физически защищенные компоненты, обеспечивающие защиту от атак, направленных на получение доступа к криптографическим ключам (как минимум ключам, используемым для получения уникального идентификатора Держателя Карты посредством хеширования или шифрования полного номера Карты), хранимым и обрабатываемым в устройстве. К таким механизмам относятся:

- защищенные процессоры (криптографические процессоры);
- защищенные микроконтроллеры (в т.ч. SAM-модули);
- защищенные Flash-накопители.

Б.1.2 Для физически защищенных компонентов должны быть выполнены настройки согласно документации вендоров соответствующих компонентов, необходимые для активации и функционирования механизмов защиты (например, механизмов стирания ключей, механизмов защиты от атак по сторонним каналам и т.д.).

Б.1.3 Для всех интегральных схем (памяти, процессоров и т.д.), которые могут быть каким-либо образом запрограммированы или сконфигурированы, необходимо отключить (без возможности повторного включения):

- любые средства, обеспечивающие проведение отладки и внутрисхемного тестирования (например, JTAG интерфейс и/или отладочные порты);
- неиспользуемые функции и программы.

Б.1.4 В Считывателе рекомендуется реализовать механизмы физической безопасности, обеспечивающие защиту от атак, направленных на вскрытие корпуса и физическое проникновение к компонентам внутри корпуса. К таким механизмам относятся:

- антивандальные крепежи и винты;
- тампер-переключатели;
- защитные экраны (сетки), расположенные на печатной плате;
- объемная герметизация с помощью эпоксидной смолы;
- использование BGA-корпусов;
- отсутствие маркировок компонентов интегральной схемы.

Б.2 Защита криптографических ключей

Б.2.1 Криптографические ключи, используемые для (1) получения уникального идентификатора Держателя Карты посредством хеширования полного номера Карты, секретные и закрытые ключи, используемые для (2) получения уникального идентификатора Держателя Карты посредством шифрования полного номера Карты, (3) шифрования данных Карт, (4) защиты сетевого взаимодействия и (5) защиты аутентификационных данных при их хранении в устройстве, должны быть защищены от модификации, подмены и раскрытия.

Б.2.2 Открытые ключи, используемые для (1) защиты сетевого взаимодействия и (2) проверки подлинности прошивки Считывателя и других данных, должны быть защищены от модификации и подмены.

Б.3 Защита данных Карт

Б.3.1 Прием данных Карт должен осуществляться только через интерфейс бесконтактного считывателя.

Б.3.2 Данные Карт в открытом виде после считывания должны быть сразу зашифрованы или переданы на компонент Считывателя, выполняющий их преобразование для дальнейшего использования в Нефинансовом сервисе.

Б.3.3 Данные Карт в открытом виде не должны передаваться за пределы Считывателя.

Б.3.4 В любой момент времени в памяти Считывателя не должны одновременно обрабатываться данные более одной Карты[11].

Б.3.5 Данные Карт должны надежно удаляться из постоянной и временной памяти Считывателя сразу после получения уникального идентификатора Держателя Карты посредством хеширования или шифрования полного номера Карты.

Б.3.6 Данные Карт должны очищаться из всех мест хранения, включая локальные переменные (перед выходом из функции) и регистры.

Б.3.7 Функция очистки буферов не должна быть удалена в процессе оптимизации компилятора или других средства оптимизации кода (при наличии).

[11] Требование не относится к идентификаторам Держателя Карты, полученным после хеширования или шифрования полного номера Карты.

Б.4 Проведение самотестирования

Б.4.1 Должно проводиться самотестирование Считывателя, включающее в себя проверку целостности и подлинности своей ОС/прошивки.

Б.4.2 Самотестирование должно автоматически выполняться при включении питания (например, после выключения питания, прерывания питания или перезагрузки) и далее не реже одного раза в 24 часа.

Б.4.3 В случае обнаружения ошибки в процессе самотестирования должны отключаться все функции Считывателя, связанные с выполнением криптографических операций и обработкой данных Карт, включая их ввод.

Б.5 Обновление ОС/прошивки

Б.5.1 Считыватель должен поддерживать обновление своей ОС/прошивки.

Б.5.2 Считыватель должен проводить криптографическую проверку целостности и подлинности устанавливаемых обновлений.

Б.5.3 Если при установке обновления его целостность и подлинность не подтверждаются, то обновление должно отклоняться и удаляться.

Б.6 Безопасная настройка ОС/прошивки

Б.6.1 ОС/прошивка Считывателя должна содержать только программное обеспечение (компоненты, сервисы и службы), минимально необходимое для работоспособности устройства.

Б.6.2 ОС/прошивка должна быть настроена безопасно и работать с минимальными привилегиями.

Б.6.3 Не допускается установка в Считыватель дополнительных приложений, изменяющих или расширяющих функциональность ОС/прошивки устройства, разработанную производителем устройства.

Б.6.4 Рекомендуется реализовать средствами ОС и/или процессора Считывателя механизмы защиты, такие как ASLR/KASLR, Stack Canaries, NX bit, PIC/PIE, RELRO, SMEP/SMAP, config_strict_devmem.

Б.7 Защита критичных сервисов

Б.7.1 При получении доступа к критичным сервисам[12] должна осуществляться аутентификация с использованием аутентификационных данных (например, пароля/кода аутентификации).

Б.7.2 Аутентификационные данные должны быть защищены от модификации, подмены и раскрытия.

Б.7.3 Пароли/коды аутентификации должны состоять не менее чем из семи символов или иметь эквивалентную сложность (энтропию).

Б.7.4 Должны быть установлены ограничения на количество запросов к критичным сервисам, ограничения на попытки получения доступа и ограничения на период времени, при превышении которых Считыватель принудительно возвращается в нормальный режим работы.

Б.8 Требования к ГСЧ и ГПСЧ

Для генерации случайных чисел, связанных с защитой данных Карт или с безопасностью Считывателя, должен использоваться ГСЧ и/или ГПСЧ, который обеспечивает:

- достаточную непредсказуемость генерируемых чисел;
- статистическую безопасность;
- большой период генерируемой последовательности.

Б.9 Криптографические алгоритмы и управление ключами

Б.9.1 При реализации в Считывателе методов шифрования (включая шифрование полного номера Карты) и аутентификации должны использоваться стойкие криптографические алгоритмы с эффективной длиной ключа не менее 128 бит для симметричных алгоритмов, 2048 бит для асимметричных алгоритмов, 224 бит для алгоритмов на основе эллиптических кривых. Разрешено использование криптографических алгоритмов AES-128, AES-192, AES-256, ГОСТ Р 34.12-2015, RSA-2048, ECDSA-224[13], ГОСТ Р 34.10-2012.

[12] Критичные сервисы – это сервисы, которые позволяют выполнять недоступные при обычном использовании устройства критичные функции. Например, сервис загрузки ключей, изменения конфигурации устройства или смены аутентификационных данных.

[13] Для перечисленных ассиметричных алгоритмов RSA и ECDSA допускается использование ключей большей длины.

Б.9.2 Для хеширования полного номера Карты в Считывателе могут использоваться только алгоритмы HMAC с секретным ключом, реализованные на основе следующих функций хеширования: ГОСТ Р 34.11-2012, SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512), SHA-3 (SHA3-224, SHA3-256, SHA3-384, SHA3-512).

Б.9.3 Управление любыми секретными и закрытыми ключами, а также ключами хеширования, используемыми в Считывателе, должно соответствовать следующим требованиям:

- секретные и закрытые ключи, не используемые для получения уникального идентификатора Держателя Карты, должны быть уникальны для каждого Считывателя;
- должен соблюдаться принцип использования ключей только в соответствии с назначением этих ключей.

Б.10 Требования к интерфейсам и внешнему взаимодействию

Б.10.1 Для всех поддерживаемых Считывателем логических и физических интерфейсов (включая, но не ограничиваясь, USB-порт, COM-порт, TCP/IP интерфейс) должны быть выполнены следующие требования:

- должны поддерживаться задокументированные команды;
- должны отсутствовать аутентификационные данные «по умолчанию», установленные производителем, и тестовые данные и/или параметры;
- должны быть реализованы механизмы защиты от распространенных атак, таких как: (1) атаки на данные и структуры данных, реализуемые путем эксплуатации уязвимостей, возникающих при некорректном выделении памяти, отсутствии обработки исключений, переполнении буфера и т.д.; (2) атаки внедрения кода; (3) атаки на реализации криптографических алгоритмов; (4) атаки на механизмы контроля доступа, включая попытки обхода механизмов идентификации, аутентификации или авторизации.

Б.10.2 Если в Считывателе реализован сетевой интерфейс для взаимодействия по сети, то должен поддерживаться протокол TLS 1.2 или выше.

Б.10.3 Реализованные в Считывателе протоколы для защиты сетевого взаимодействия должны обеспечивать:

- конфиденциальность;
- целостность;

- взаимную аутентификацию Считывателя и сервера;
- защиту от повторного воспроизведения[14].

Б.10.4 Реализованные в Считывателе протоколы для защиты сетевого взаимодействия должны использовать описанные в подразделе Б.9 криптографические алгоритмы, минимальные длины ключей и функции хеширования.

Б.10.5 Полученные пакеты данных с некорректной подписью должны отклоняться Считывателем.

Б.10.6 Wi-Fi соединение должно быть безопасно настроено. Должно быть обеспечено шифрование данных, получаемых и передаваемых через Wi-Fi интерфейс. Это шифрование должно дополнять любое другое шифрование, реализованное в Считывателе.

Б.10.7 Bluetooth соединение должно быть защищено от прослушивания и атак типа «человек посередине». Должно быть обеспечено шифрование данных, получаемых и передаваемых через Bluetooth интерфейс. Это шифрование должно дополнять любое другое шифрование, реализованное в Считывателе.

Б.11 Требования к среде и процессам обеспечения безопасности на этапах разработки и производства Считывателя

Б.11.1 Должны быть определены, разработаны и реализованы требования и процедуры обеспечения безопасности в рамках процесса разработки ОС/прошивки Считывателя.

Б.11.2 Должно быть обеспечено выполнение анализа программного кода ОС/прошивки Считывателя и тестирования на предмет отсутствия ошибок и уязвимостей. Все выявленные ошибки и уязвимости должны быть устранены перед передачей программного кода в промышленную эксплуатацию.

Б.11.3 Программный код ОС/прошивки Считывателя должен храниться в выделенном для этой цели защищенном репозитории.

Б.11.4 Должно быть обеспечено безопасное компилирование программного кода ОС/прошивки Считывателя.

Б.11.5 Должен быть обеспечен контроль целостности скомпилированного кода ОС/прошивки Считывателя с помощью выполнения электронной подписи ОС/прошивки устройства.

[14] Например, путем использования счетчиков или одноразовых номеров (nonces).

Б.11.6 Должны быть определены, разработаны и реализованы требования и процедуры по обеспечению физической, логической безопасности, а также безопасности при управлении персоналом для обеспечения защищенности дизайна и реализации компонентов Считывателя.

Б.11.7 Если на этапе производства и/или обслуживания выполняется ввод в Считыватель критичных данных (криптографических ключей и/или аутентификационных данных), ввод должен производиться в защищенном помещении авторизованными для этого сотрудниками при соблюдении принципа двойного контроля.

Приложение В. Перечень требований по безопасности к среде обработки данных Карт

В.1 Хранение данных Карт должно быть минимизировано с помощью реализации следующих мер:

- определение и учет всех мест обработки и хранения данных Карт;
- ограничение времени хранения данных Карт в мере, необходимой для реализации целей их хранения;
- реализация удаления данных Карт после достижения целей их хранения и истечения установленного срока их хранения;
- выполнение периодических проверок того, что данные Карт, для которых были достигнуты цели их хранения и истек срок их хранения, были удалены без возможности восстановления и /или использования.

В.2 В Организации должны быть реализованы меры по защите данных Карт на сетевом уровне, включая размещение системы, в которой обрабатываются и/или хранятся данные Карт, в выделенном сетевом сегменте (далее – Сегмент данных Карт), доступ в который контролируется с помощью системы межсетевого экранирования. Должны быть разрешены только входящие и исходящие соединения с системами в Сегменте данных Карт, минимально необходимые для выполнения компонентами в Сегменте данных Карт их производственных задач. Запрещены любые соединения, которые не были в явном виде разрешены. Система, в которой хранятся данные Карт, должна размещаться во внутренних сетевых сегментах локальной вычислительной сети Организации и не должна размещаться в DMZ-сегментах. В Организации должна обеспечиваться антивирусная защита Сегмента данных Карт. При этом антивирусные базы должны поддерживаться в актуальном состоянии.

В.3 В Организации должна быть разработана и поддерживаться в актуальном состоянии схема сети, отражающая все соединения между Сегментом данных Карт и другими сетями.

В.4 В Организации должен быть разработан и поддерживаться в актуальном состоянии перечень аппаратных и программных системных компонентов, размещенных в Сегменте данных Карт.

В.5 Все используемые в Сегменте данных Карт сетевые сервисы, протоколы и порты должны быть идентифицированы, документированы и формально разрешены к использованию. Для всех необходимых служб, протоколов и управляющих программ, которые могут быть небезопасными, должны быть внедрены дополнительные механизмы защиты (например, SSH или TLS).

B.6 Должно выполняться шифрование любого неконсольного административного доступа ко всем программным и аппаратным ресурсам Сегмента данных Карт.

B.7 Для каждого типа используемых в Сегменте данных Карт устройств, операционных систем, систем виртуализации, активного сетевого оборудования, систем управления базами данных и прикладного программного обеспечения, настройки которых способны повлиять на безопасность данных Карт, должны быть разработаны и внедрены стандарты безопасной настройки, учитывающие известные уязвимости и отраслевые рекомендации по обеспечению безопасности.

B.8 При передаче данных Карт по открытым каналам связи должны применяться средства, протоколы и алгоритмы, обеспечивающие защиту передаваемых данных и соответствующие следующим требованиям:

- используются только безопасные версии (например, версия 1.2 или выше протокола TLS, версия 2 протокола SSH) и конфигурации средств и протоколов защиты;
- используются только доверенные ключи и сертификаты;
- используются стойкие алгоритмы шифрования и аутентификации с длиной ключа не менее 128 бит для симметричных алгоритмов, 2048 бит для асимметричных алгоритмов, 224 бит для алгоритмов на основе эллиптических кривых. Примерами таких алгоритмов являются: ГОСТ Р 34.12-2015, AES-128, AES-192, AES-256, RSA-2048, ECDSA-224;
- используются стойкие алгоритмы хеширования. Примерами таких алгоритмов являются ГОСТ Р 34.11-2012, SHA-256, SHA-384 или SHA-512. Не рекомендуется использование алгоритмов MD4/5 и SHA1, которые являются устаревшими.

B.9 Не реже одного раза в квартал в Организации должно осуществляться внешнее и внутреннее инструментальное сканирование ресурсов в Сегменте данных Карт на предмет наличия известных уязвимостей. Выявленные в ходе сканирования уязвимости должны быть оперативно устранены.

B.10 Рекомендуется проводить периодическое (например, ежегодное) тестирование на проникновение в Сегмент данных Карт.

B.11 Каждому пользователю систем в рамках Сегмента данных Карт должен быть назначен уникальный идентификатор (имя учетной записи). Все учетные записи (включая системные, служебные и учетные записи пользователей и администраторов) в системном и

прикладном программном обеспечении Сегмента данных Карт должны быть защищены стойкими методами аутентификации. При этом должно выполняться следующее:

- минимальная длина паролей должна составлять не менее 8 символов. Пароли должны содержать цифры и буквы;
- блокирование учетной записи при превышении установленного числа попыток неправильного ввода пароля (не более 10 попыток). Период блокировки должен составлять не менее 30 минут или учетные записи должны разблокированы после подтверждения личности пользователя;
- пароли должны быть защищены при передаче и хранении с помощью стойких криптографических алгоритмов;
- при превышении тайм-аута неактивности пользователя должна выполняться автоматическая блокировка сеанса доступа к системному компоненту. Возможность продолжения работы пользователя с системой должна быть обеспечена после повторного прохождения аутентификации (повторном запросе пароля пользователя);
- при удаленном и неконсольном административном доступе в Сегмент данных Карт рекомендуется использовать многофакторную (двухфакторную) аутентификация. Используемый механизм многофакторной аутентификации должен быть защищен от атак повторного воспроизведения;
- при использовании встроенных учетных записей на системных компонентах (устройства, серверы, СУБД, сетевое оборудование, средства виртуализации, прикладное программное обеспечение, средства защиты информации) не допускается использование паролей, установленных производителем по умолчанию;
- использование разделяемых между несколькими администраторами системных и служебных учетных записей должно быть возможно только в случае наличия обоснованной и документированной производственной необходимости, и формального разрешения к использованию;
- при увольнении работника принадлежащие ему учетные записи незамедлительно блокируются.

В.12 Доступ к данным Карт и системным компонентам в Сегменте данных Карт должен быть ограничен и предоставляться в соответствии со служебной необходимостью. Должен выполняться периодический (не реже 1 раза в 6 месяцев) пересмотр назначенных прав доступа.

В.13 Должны быть реализованы меры по ограничению физического доступа к компонентам системы, в которой хранятся и/или обрабатываются данные Карт, и носителям данных Карт.

В.14 Должны быть реализованы меры по ограничению доступа к съемным носителям данных Карт.

В.15 В рамках Сегмента данных Карт должна обеспечиваться регистрация следующих событий:

- события доступа к данным Карт, хранимым в Организации;
- действия пользователей с административными привилегиями;
- неудачные попытки доступа;
- изменение параметров аутентификации, включая создание новых учетных записей; расширение привилегий учетных записей; любые события изменения, добавления, удаления учетных записей с административными привилегиями;
- изменение параметров регистрации событий, включая остановку и запуск подсистем ведения журналов регистрации событий.

В.16 Должен проводиться периодический анализ журналов регистрации событий. Для обеспечения полноты и эффективности анализа журналов регистрации событий рекомендуется использовать систему управления событиями ИБ.

В.17 Должен обеспечиваться мониторинг и выявление в инфраструктуре Организации инцидентов информационной безопасности, которые привели или могут привести к компрометации данных Карт (далее – Инцидент ИБ).

В.18 В случае выявления подозрения на Инцидент ИБ, должно проводиться его обработка: локализация инцидента, расследование причин возникновения инцидента, устранение последствий инцидента.

В.19 В Организации должен быть разработан план реагирования на Инциденты ИБ, который содержит:

- последовательность действий по локализации и устранению последствий Инцидента ИБ;
- перечень лиц, ответственных за реагирование.