СОГЛАСОВАНО	**УТВЕРЖДАЮ**
Заместитель Председателя Банка России	Первый заместитель руководителя Научно-технической службы ФСБ России
_____ Д.Г. Скобелкин	_____ А.М. Ивашко
«15» 01 2020 г.	«24» 01 2020 г.

ТРЕБОВАНИЯ К СРЕДСТВАМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ПЛАТЕЖНЫХ УСТРОЙСТВАХ С ТЕРМИНАЛЬНЫМ ЯДРОМ, СЕРВЕРНЫХ КОМПОНЕНТАХ ПЛАТЕЖНЫХ СИСТЕМ (HSM МОДУЛЯХ), ПЛАТЕЖНЫХ КАРТАХ И ИНЫХ ТЕХНИЧЕСКИХ СРЕДСТВАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПЛАТЕЖНОЙ СИСТЕМЫ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ, УКАЗАННЫХ В ПУНКТЕ 2.20 ПОЛОЖЕНИЯ БАНКА РОССИИ ОТ 9 ИЮНЯ 2012 Г. № 382-П

№ ФТ-56-3/32
28.02.2020

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Введение

Настоящие требования разработаны и утверждены в рамках мероприятий федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»: 05.02.002.017.004 - «Разработка и опубликование требований к СКЗИ, указанных в пункте 2.20 положения Банка России от 9 июня 2012 г. № 382-П (в редакции указания Банка России от 7 мая 2018 г. № 4793-У).».

Настоящий документ определяет требования Российской Федерации по информационной безопасности к техническим средствам и программному обеспечению, реализующим криптографические механизмы в:

- платежных устройствах с терминальным ядром (терминалы и банкоматы),
- аппаратных модулях безопасности информационной инфраструктуры платежных систем (HSM модулях),
- платежных картах,
- иных технических средствах информационной инфраструктуры платежной системы.

СКЗИ для использования в платежных устройствах с терминальным ядром (терминалы и банкоматы), аппаратных модулях безопасности информационной инфраструктуры платежных систем (HSM модулях), платежных картах и иных технических средствах информационной инфраструктуры платежной системы, должны разрабатываться в соответствии с Положением ПКЗ-2005, утвержденным Приказом ФСБ России от 9 февраля 2005 года № 66 (зарегистрирован в Минюсте РФ 3 марта 2005 г., регистрационный № 6382).

Предельные числовые значения рассматриваемых в настоящих требованиях механизмов безопасности, определяются ФСБ России.

Методики подтверждения указанных в настоящих требованиях свойств и обеспечения противодействия указанным в настоящих требованиях атакам согласуются с ФСБ России.

1.2. Список используемых сокращений

В настоящих требованиях применяются следующие термины с соответствующими определениями:

Термин/Сокращение	Определение
Платежное устройство с терминальным ядром (платежный терминал/банкомат)	Программно-аппаратный комплекс или его части, предназначенный для выполнения операций с использованием платёжных карт, в том числе осуществления переводов денежных средств, выдачи и приема наличных денежных средств
Аппаратный модуль безопасности информационной инфраструктуры платежных систем (HSM модуль), HSM	Программно-аппаратный комплекс или его части, предназначенный для выполнения криптографических преобразований при проведении платежных операций, управления ключами шифрования и(или) шифрования данных платежных карт, персонализации платежных карт при эмиссии
Платежная карта	Программно-аппаратный комплекс или его части, предназначенный для обеспечения формирования платежных поручений, находящийся у клиента банка.
ПИН, ПИН-код, персональный идентификационный номер – (PIN, personal identification number)	Секретный цифровой пароль, известный только держателю платежной карты или владельцу платежной карты и эмитенту, используемый для аутентификации пользователя
PAN	Номер платежной карты, отображенный на ее лицевой или обратной стороне
Устройство для ввода ПИН – (PIN pad)	Вид платежного терминала, предназначенный только для ввода ПИН

Защищаемая информация	Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями нормативно правовых документов или требованиями, устанавливаемыми собственником информации
Код верификации карты	Трёхзначный код проверки подлинности платёжной карты
СФ	Среда функционирования СКЗИ
АС СФ	Аппаратные средства среды функционирования СКЗИ
АС СКЗИ	Аппаратные средства СКЗИ
ПО АС СКЗИ	Программное обеспечение аппаратных средств среды функционирования СКЗИ
ПО СКЗИ	Программное обеспечение СКЗИ
ПО СФ СКЗИ	Программное обеспечение среды функционирования СКЗИ
ИС	Информационная система
ФДСЧ	Физический датчик случайных чисел
ПДСЧ	Программный датчик случайных чисел
ТКУИ	Технические каналы утечки информации

В дополнение к указанному списку следует руководствоваться терминами и определениями из документа Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации» и Положения ПКЗ-2005.

2. ОПИСАНИЕ МОДЕЛИ НАРУШИТЕЛЯ ДЛЯ СКЗИ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

2.1. Сведения, используемые при создании способов, подготовке и проведении атак

СКЗИ должны противостоять атакам, при создании которых используются следующие сведения:

а) Сведения о СКЗИ

- общие сведения об информации, используемой в процессе эксплуатации СКЗИ;
- защищенная СКЗИ информация;
- все данные, передаваемые по каналам связи, не защищенным от несанкционированного доступа к информации организационно-техническими мерами;
- сведения, получаемые в результате анализа информативных сигналов;
- документированные и опубликованные возможности ПО СКЗИ, ПО АС СКЗИ и АС СКЗИ;
- исходные коды ПО СКЗИ и ПО АС СКЗИ[1];
- содержание конструкторской документации на СКЗИ, в том числе сведения о мерах защиты от внешних воздействий;
- сведения обо всех нарушениях правил пользования СКЗИ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации

[1] Для аппаратных модулей безопасности информационной инфраструктуры платежных систем сведения, содержащиеся в исходных текстах ПО СФ и ПО АС СФ.

организационно-техническими мерами;

- сведения обо всех неисправностях и сбоях АС СКЗИ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами.

б) Сведения о СФ (АС СФ)

- содержание документации на СФ;
- опубликованные возможности и уязвимости ПО СФ, ПО АС СФ и АС СФ;
- сведения обо всех нарушениях правил эксплуатации СФ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами;
- сведения обо всех неисправностях и сбоях АС СФ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами.

в) Сведения о платежной информационной системе (ИС)

- общие сведения об ИС, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы ИС;
- документированные и опубликованные сведения об информационных технологиях, базах данных, АС, ПО, используемых в ИС совместно с СКЗИ[2];
- сведения обо всех сетях связи в составе ИС, работающих на

---

[2] Для аппаратных модулей безопасности информационной инфраструктуры платежных систем о недекларированных возможностях ПО СФ и неопубликованных уязвимостях ПО СФ.

едином криптографическом ключе[3].

2.2. Технические средства, используемые при создании способов, подготовке и проведении атак

СКЗИ должны противостоять атакам, реализуемым посредством использования следующих средств:

а) штатные средства СКЗИ (ПО СКЗИ, АС СКЗИ, СФ СКЗИ);

б) специально разработанные АС и ПО;

в) средства перехвата и проведения исследований информативных сигналов;

г) средства, эксплуатирующие для несанкционированного доступа недекларированные (недокументированные) возможности и уязвимости ПО[4].

2.3. Формы доступа, используемые при создании способов, подготовке и проведении атак

СКЗИ должны противостоять атакам, проводящимся из-за пределов контролируемой зоны, посредством целенаправленного пассивного и/или активного воздействия на каналы связи технических средств информационной инфраструктуры платежной системы, устройства питания.

СКЗИ должны противостоять атакам, проводящимся нарушителем, имеющим непосредственный доступ к техническим средствам информационной

---

[3] Для аппаратных модулей безопасности информационной инфраструктуры платежных систем, содержащиеся в конструкторской документации на информационные технологии, базы данных, ПО, используемые в ИС совместно с СКЗИ.

[4] Для платежных карт в дополнение к заявленному - измерительное и аналитическое оборудование для подготовки и проведения атак на СКЗИ, включающее: осциллограф, источники лазерного излучения (с системами позиционирования), микрозондовую станцию, климатическую камеру, двулучевые электронно-ионные системы (ФИП), средства жидкостного химического травления, установка химико-механического полирования и т.п.

инфраструктуры платежной системы, посредством попыток несанкционированного доступа, в том числе с использованием методов инженерного проникновения, с целью компрометации ключа или искажения ПО СФ СКЗИ, АС СФ СКЗИ, ПО СКЗИ, АС СКЗИ и протоколов взаимодействия карты с платежным устройством и HSM с платежным устройством[5].

[5] Для аппаратных модулей безопасности информационной инфраструктуры платежных систем необходимо обеспечить защиту ключевой информации пользователей от администратора (привилегированного пользователя) модуля.

3. ОБЩИЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СКЗИ В ТЕХНИЧЕСКИХ СРЕДСТВАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПЛАТЕЖНОЙ СИСТЕМЫ

СКЗИ должно обеспечивать безопасность защищаемой информации при реализации атак в процессе обработки защищаемой информации в технических средствах информационной инфраструктуры платежной системы и/или при условии несанкционированного доступа к защищенной СКЗИ информации в процессе ее хранения или передачи по каналам связи.

При проектировании комплекса средств защиты технических средств информационной инфраструктуры платежной системы необходимо применять эшелонированный подход, что означает, что выход из строя или нарушение работы одного механизма обеспечения безопасности технического средства информационной инфраструктуры платежной системы не должен приводить выходу из строя других механизмов защиты.

К конфиденциальным данным относятся: PIN-код, код верификации, ключи шифрования, ключи аутентификации, закрытые ключи, а также в некоторых случаях PAN.

Если используется дистанционное распределение ключей, то устройство должно поддерживать взаимную аутентификацию между отправляющим хостом распространения ключей и принимающим устройством.

Симметричные и закрытые ключи, которые находятся внутри технического средства информационной инфраструктуры платежной системы для обеспечения шифрования данных учетной записи, должны быть уникальными для каждого устройства.

В ТЗ на разработку (модернизацию) СКЗИ могут предъявляться дополнительные требования к СКЗИ, не противоречащие принципам настоящего документа.

СКЗИ считается прошедшим оценку соответствия требованиям, если для ввода СКЗИ в эксплуатацию не требуется проведение дополнительных тематических исследований СКЗИ после утверждения положительного заключения ФСБ России о соответствии СКЗИ всем предъявляемым к нему требованиям.

В отдельных случаях, при наличии соответствующего обоснования по решению Банка России и ФСБ России может быть разрешена эксплуатация СКЗИ, когда отдельные положения требований по безопасности информации к ним не выполнены.

4. ПРИНЦИПЫ ПРИМЕНЕНИЯ КРИПТОГРАФИЧЕСКИХ МЕХАНИЗМОВ ЗАЩИТЫ

4.1. Применение криптографических механизмов

Применение криптографических механизмов в СКЗИ основывается на следующих принципах:

- При разработке (модернизации) СКЗИ должны использоваться криптографические механизмы, утвержденные в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографические механизмы, имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований.
- Кроме того, с целью обеспечения совместимости с действующими криптографическими решениями должны использоваться криптографические механизмы, отвечающие международным стандартам (ISO).
- Криптографические механизмы, а также преобразования, реализующие обработку ключевой информации, ее выработку и удаление, должны быть реализованы непосредственно в СКЗИ.

4.2. Применение датчиков случайных чисел

Применение датчиков случайных чисел в СКЗИ основывается на следующих принципах:

- Датчик случайных чисел является составной частью СКЗИ и должен проходить тематические исследования совместно с СКЗИ, в котором он применяется.
- Датчик случайных чисел должен использоваться для генерации случайных (псевдослучайных) последовательностей с целью

выработки ключевой информации и/или другой случайной (псевдослучайной) информации, используемой в СКЗИ.

- При выработке ключевой информации допускается использование ФДСЧ и ПДСЧ.
- ПДСЧ, входящий в состав СКЗИ, должен использовать для выработки ключевой информации из инициализирующей последовательности криптографические механизмы, утвержденные в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографические механизмы, имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований.
- При выработке инициализирующей последовательности для ПДСЧ необходимо использовать либо ФДСЧ, реализованный в СКЗИ, либо последовательность полученную с СКЗИ, прошедшего оценку соответствия требованиям по информационной безопасности по классу КВ в соответствии с действующими требованиями к СКЗИ.

В случае выработки инициализирующей последовательности ПДСЧ на местах эксплуатации СКЗИ, необходимо:

а) в ходе тематических исследований СКЗИ провести построение, обоснование и анализ теоретико-вероятностной модели датчика случайных чисел, формирующего инициализирующую последовательность;

б) обеспечить проверку статистического качества инициализирующей последовательности ПДСЧ, осуществляемую в автоматическом режиме функционирования СКЗИ (динамический контроль);

в) реализовать механизм периодической смены инициализирующей последовательности; указанный период должен определяться и обосновываться в ходе тематических исследований СКЗИ.

В HSM для выработки первичной ключевой информации должен использоваться ФДСЧ.

Для ФДСЧ, входящих в состав СКЗИ, в ходе тематических исследований должна быть разработана теоретико-вероятностная модель используемого в ФДСЧ случайного физического процесса, а также должна быть проведена экспериментальная проверка соответствия указанной модели реализации ФДСЧ.

Для ФДСЧ на местах эксплуатации СКЗИ должна осуществляться проверка статистического качества выходной последовательности ДСЧ. Данная проверка должна осуществляться в ходе регламентных (периодических, в том числе в автоматическом режиме) проверок датчика случайных чисел (регламентный контроль) и в автоматическом режиме в процессе функционирования СКЗИ (динамический контроль).

4.3. Выработка ключевой информации

Выработка ключевой информации основывается на следующих принципах:

Выработка первичной ключевой информации должна производиться с использованием датчика случайных чисел, в том числе внешнего устройства, удовлетворяющего 4.2.

В протоколах выработки общего ключа в криптографических протоколах должны использоваться датчики случайных чисел, удовлетворяющие 4.2.

4.4. Использование ключевой информации

Использование ключевой информации в СКЗИ основывается на следующих принципах:

- Вся первичная ключевая информация должна быть выработана в соответствии с 4.3.

- В случае если ключевая информация выработана другим СКЗИ, то доведение ключевой информации до использующего ее СКЗИ должно осуществляться либо доверенным способом, либо СКЗИ, реализующим криптографическую функцию дистанционного распределения ключей по каналам связи.
- При передаче ключевой информации по каналам связи и при хранении ключевой информации и при дистанционном управлении ключевой информацией должны применяться криптографические механизмы, утвержденные в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографические механизмы, имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований.
- Используемая СКЗИ ключевая информация в незашифрованном виде должна храниться непосредственно в СКЗИ на протяжении установленного срока действия.
- Для обеспечения подлинности открытых ключей аутентификации должен использоваться механизм сертификатов открытых ключей.
- Максимальные сроки действия криптографических ключей СКЗИ должны определяться в ТЗ и уточняться в ходе проведения тематических исследований.
- В СКЗИ должен быть реализован механизм контроля срока действия криптографических ключей.

4.5. Аутентификация субъектов доступа

Аутентификация субъектов доступа основывается на следующих принципах:

В СКЗИ технических средств информационной инфраструктуры платежной системы должны быть реализованы криптографические механизмы,

удовлетворяющие 4.1 и обеспечивающие аутентификацию субъектов и/или процессов доступа, осуществляющих доступ или взаимодействующих с СКЗИ.

При этом для обеспечения удаленной аутентификации при организации защищенной передачи данных и для обеспечения аутентификации при взаимодействии с СКЗИ по каналам удаленного управления должны применяться криптографические механизмы, утвержденные в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографические механизмы, имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований.

Использование паролей для аутентификации субъектов доступа (пользователей), являющихся физическими лицами и осуществляющих доступ к техническим средствам информационной инфраструктуры платежной системы, допускается только для локальной аутентификации СКЗИ.

Для проведения локальной аутентификации с целью изменения настроек безопасности, а также загрузки/смены/уничтожения ключей (администрирования) требуется использовать:

- в платежных устройствах с терминальным ядром (терминалах) не менее двух паролей.

- в банкоматах, аппаратных модулях безопасности информационной инфраструктуры платежных систем (HSM модулях) и иных технических средствах информационной инфраструктуры платежной системы как минимум два аутентифицирующих фактора (знание, владение).

Для обеспечения локальной аутентификации субъектов доступа, являющихся физическими лицами и осуществляющих доступ к СКЗИ в аппаратных модулях безопасности информационной инфраструктуры платежных систем (HSM модулях), должна быть реализована ролевая аутентификация субъектов доступа. При этом требуется поддержка следующих ролей:

- роль пользователя, в рамках которой выполняются реализованные в СКЗИ криптографические функции;
- роль привилегированного пользователя, в рамках которой могут выполняться функции управления СКЗИ (настройка, конфигурирование и т.п.).

Кроме того, в HSM критические функции управления ключами должны выполняться под двойным контролем (т. е. при условии обязательной аутентификации не менее двух привилегированных пользователей). К критическим функциям управления ключами в обязательном порядке должны относиться функции формирования (загрузки) и резервирования локальных мастер-ключей HSM, предназначенных для защищенного хранения ключей держателей карт.

При аутентификации субъектов доступа, являющихся процессами и осуществляющих взаимодействие с СКЗИ, должен быть реализован криптографический механизм взаимной аутентификации.

Для всех классов СКЗИ для любого реализованного механизма аутентификации субъектов доступа должен быть реализован механизм ограничения числа следующих подряд неудачных попыток аутентификации одного субъекта доступа.

При превышении числа следующих подряд неудачных попыток аутентификации одного субъекта доступа установленного предельно допустимого значения доступ этого субъекта доступа к СКЗИ следует блокировать на заданный промежуток времени.

4.6. Имитозащита

Реализация имитозащиты в СКЗИ должна основываться на следующих принципах:

- Криптографические механизмы, обеспечивающие имитозащиту информации, должны удовлетворять требованиям 4.1.

- Для обеспечения имитозащиты каналов управления и передачи данных по каналу связи должны применяться криптографические механизмы, утвержденные в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографические механизмы, имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований.
- Допускается использование усиленной электронной подписи для обеспечения имитозащиты передаваемых сообщений.

5. ПРИНЦИПЫ ПРИМЕНЕНИЯ ИНЖЕНЕРНО-КРИПТОГРАФИЧЕСКИХ МЕХАНИЗМОВ ЗАЩИТЫ

5.1. Применение инженерно-криптографических механизмов

Использование инженерно-криптографических механизмов в СКЗИ основывается на следующих принципах:

- Инженерно-криптографическая защита СКЗИ должна исключить опасные события, возникающие вследствие неисправностей или сбоев АС СКЗИ и АС СФ и приводящие к возможности осуществления успешных атак на СКЗИ и технические средства информационной инфраструктуры платежной системы.
- Инженерно-криптографическая защита СКЗИ должна предусматривать защиту от возможных непреднамеренных действий пользователя/администратора, не предусмотренных правилами пользования СКЗИ и приводящих к возможности осуществления успешных атак на СКЗИ.
- В качестве составной части СКЗИ должна быть реализована система защиты от несанкционированного доступа к используемой СКЗИ ключевой и криптографически опасной информации. Также в качестве составной части СКЗИ должна быть реализована система защиты от несанкционированного доступа к защищаемой СКЗИ информации.
- В ходе тематических исследований СКЗИ должны быть определены технические характеристики СКЗИ и их предельные значения, позволяющие обеспечить выполнение предъявляемых к СКЗИ требований.
- В СКЗИ должен быть реализован контролирующий механизм, сигнализирующий или блокирующий работу СКЗИ при достижении предельных значений технических характеристик СКЗИ.

В СКЗИ должна предусматриваться реализация блокирования работы СКЗИ:

- Блокировка СКЗИ должна осуществляться в случаях диагностики неисправности СКЗИ, при достижении предельных значений технических характеристик СКЗИ, при истечении срока действия ключей, нарушении целостности ПО СКЗИ[6].
- При блокировке СКЗИ должна обеспечиваться невозможность выхода защищаемой и криптографически опасной информации в канал связи.
- Перечень случаев, когда блокировка СКЗИ является обязательной, уточняется в ходе проведения тематических исследований.
- Промежуток времени, в течение которого блокируется работа СКЗИ, определяется заказчиком СКЗИ и уточняется в ходе проведения тематических исследований.

В начале работы СКЗИ (включении питания) следует производить диагностический контроль работоспособности мер криптографической и инженерно-криптографической защиты (или контроль целостности).

Для СКЗИ, реализованного в технических средствах информационной инфраструктуры платежной системы, должен быть обеспечен контроль целостности СКЗИ на этапах хранения, транспортирования, ввода в эксплуатацию и эксплуатации жизненного цикла СКЗИ, а также контроль целостности СФ на этапе эксплуатации жизненного цикла СКЗИ с использованием криптографических механизмов контроля целостности. Перечень объектов среды функционирования СКЗИ, контроль целостности которых осуществляется СКЗИ, определяется и обосновывается в ходе проведения тематических исследований. Контроль целостности следует

---

[6] Конкретный набор параметров при достижении, которых должна производится блокировка и уточняется на этапе ТИ и их экспертизы.

проводить до начала обработки информации, безопасность которой должна обеспечиваться СКЗИ.

Для СКЗИ должен быть реализован периодический контроль целостности. Период контроля определяется и обосновывается в ходе тематических исследований СКЗИ. В случае обнаружения нарушения целостности следует осуществлять блокировку СКЗИ.

В состав СКЗИ должен входить механизм, обеспечивающий контроль целостности ключевой и исходной ключевой информации.

Для СКЗИ в составе аппаратных модулей безопасности информационной инфраструктуры платежных систем (HSM) контроль целостности должен осуществляться только с использованием криптографических механизмов. Механизм контроля целостности должен включать средства контроля собственной корректной работы.

В состав СКЗИ должны входить компоненты, обеспечивающие очистку областей памяти, используемых СКЗИ для хранения защищаемой, ключевой, исходной ключевой и криптографически опасной информации, при освобождении и/или перераспределении областей памяти, путем записи в области памяти случайной информации, вырабатываемой датчиком случайных чисел.

В СКЗИ следует реализовывать следующий механизм регистрации событий:

- В состав СКЗИ должен входить модуль, производящий регистрацию в электронном журнале регистрации событий в СКЗИ и СФ, связанных с выполнением СКЗИ определенных в ТЗ криптографических функций.
- В перечень регистрируемых событий, в частности, должны входить:
    - факты ввода, смены и стирания ключевой информации;
    - факты срабатывания блокировки СКЗИ по причине исчерпывания ключевой информации;

- факты окончания срока действия криптографических ключей;
- факты повторного ввода ключей;
- факты срабатывания системы защиты от несанкционированного доступа к информации;
- результаты контроля целостности ПО СКЗИ;
- факты проведения регламентных работ.

- Перечень событий, регистрируемых в журнале регистрации событий, может уточняться в ходе проведения тематических исследований.
- Должен быть реализован криптографический контроль целостности журналов регистрации событий.
- Очистка журнала должна производиться доверенным лицом только после архивирования, после чего первой записью в журнале должна быть запись об очистке/архивировании журнала[7].

5.2. Базовые положения для программного обеспечения СКЗИ

Для проведения тематических исследований ПО СКЗИ для всех классов должно быть представлено в виде исходных текстов, исполняемого кода и документации.

Исходные тексты ПО СКЗИ должны удовлетворять следующим условиям:

а) исходные тексты ПО СКЗИ должны быть оформлены в соответствии с ГОСТ 19.401. При этом специализированная организация, проводящая тематические исследования, может

---

[7] Для СКЗИ в аппаратных модулях безопасности информационной инфраструктуры платежных систем очистка журнала должна производиться только привилегированным пользователем и только после архивирования, после чего первой записью в журнале должна быть запись об очистке/архивировании журнала. В случае невозможности переноса журнала регистрации событий в архив привилегированному пользователю может быть доступна функция стирания журнала. В этом случае СКЗИ должно обеспечивать сохранение информации о последних трех сутках работы СКЗИ, а также регистрацию факта очистки журнала с сохранением в нем даты очистки и информации о привилегированном пользователе, производившем операцию очистки.

устанавливать собственные требования к содержанию и оформлению текстов ПО СКЗИ;

б) исходные тексты ПО СКЗИ должны содержать комментарии, достаточные для понимания алгоритма функционирования ПО СКЗИ;

в) исходные тексты ПО СКЗИ должны содержать полный набор файлов, необходимый для воспроизведения из них исполняемого кода, идентичного представленному для проведения тематических исследований;

г) бинарные и ассемблерные вставки, вставки информационных массивов и входящие в состав исходных текстов фрагменты, не имеющие прямого отношения к реализации криптографических функций СКЗИ, должны быть документированы и обоснованы.

Документация на ПО СКЗИ должна включать в себя:

а) спецификацию ПО СКЗИ;

б) описание ПО СКЗИ;

в) описание применения ПО СКЗИ;

г) пояснительную записку.

Подача на вход любых значений параметров экспортируемых функций ПО СКЗИ не должна приводить к появлению уязвимостей, позволяющих реализовывать успешные атаки на СКЗИ.

В случае выявления при проведении тематических исследований значений параметров экспортируемых функций ПО СКЗИ, приводящих к появлению уязвимостей, позволяющих реализовывать успешные атаки на СКЗИ, составляется список таких функций и значений параметров. Этот список исключается из документации на СКЗИ, представляемой разработчикам, осуществляющим встраивание СКЗИ в ИС. Действие заключения о соответствии СКЗИ требованиям по информационной безопасности ФСБ России на функции из указанного списка не распространяется.

5.3. Положения по соответствию ПО СФ СКЗИ

Операционная система устройства должна содержать только программное обеспечение (компоненты и службы), необходимое для осуществления платежных операций и обеспечения сопутствующих функций, а также целевых функций, заявленных в ТЗ на разработку и проведение тематических исследований (ТИ). Операционная система должна быть настроена и надежно работать с минимальными привилегиями.

Дополнительные модули или приложения (например, программы лояльности) могут быть установлены в ПО СФ СКЗИ только после проведения оценки влияния данных модулей/приложений на СКЗИ.

Для СКЗИ аппаратных модулей безопасности информационной инфраструктуры платежных систем (HSM модулей) на ТИ предоставляются исходные коды ПО СФ СКЗИ.

Системное программное обеспечение не должно содержать модулей, использующих технологию аппаратной виртуализации физических ресурсов.

Если техническое средство информационной инфраструктуры платежной системы поддерживает несколько модулей/приложений, оно должно принудительно осуществлять разделение ресурсов между модулями/приложениями. Должен быть исключен сценарий, когда одно приложение препятствует или изменяет другое приложение или ОС устройства, включая, но не ограничиваясь, изменением объектов данных и кода, являющимися частью другого приложения или ОС.

Техническое средство информационной инфраструктуры платежной системы должно обеспечивать защиту от сетевых атак на программные интерфейсы ввода-вывода.

Для удаленного управления, мониторинга и контроля должны использоваться прикладные протоколы, работающие поверх транспортного протокола передачи данных.

ПО СФ СКЗИ должно быть разработано с таким расчетом, что защищаемая информация должна храниться не дольше и использоваться не чаще, чем это необходимо.

Средства криптографической защиты информации, реализованные в платежных устройствах с терминальным ядром должны быть предназначены для использования в операционной среде устройства с терминальным ядром (операционная система должна являться средой функционирования СКЗИ).

Должна быть проведена оценка влияния программного обеспечения СФ на СКЗИ.

Должна быть обоснована замкнутость программной среды ПО СФ СКЗИ, которая должна обеспечивать:

а) исключение попадания и запуска в ОС программ, не входящих в состав ПО СФ СКЗИ;

б) исключение доступа к СКЗИ любым способом по незащищенным (криптографическим способом с использованием криптографических механизмов, утвержденных в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографических механизмов, имеющих положительное заключение ФСБ России по результатам их экспертных криптографических исследований) протоколам.

в) исключение доступа к СКЗИ неавторизованных пользователей и процессов.

5.4. Положения для аппаратных средств СКЗИ

Использование АС СКЗИ (если в СКЗИ входят АС СКЗИ) должно быть исследовано на соответствие заданным законам функционирования по электрическим принципиальным схемам или их эквивалентам.

5.5. Положения по физической защите СКЗИ и СФ СКЗИ

Все СКЗИ должны предусматривать защитные меры от физического проникновения с целью деструктивного воздействия (например, компрометации ключевой информации и т.п.), такого как (например) сверление, воздействие лазером или химическими веществами, вскрытие корпуса, проникновение через любые отверстия в корпусе, установка устройств перехвата ПИН и т.п.

Для платежных карт должны быть реализованы следующие меры защиты, входящие в АС СКЗИ:

а) активный защитный экран (сетка), обеспечивающий защиту от физического проникновения к логическим элементам, защиту от оптического зондирования (анализа топологии) и контроля целостности путем пропускания по шинам защитного экрана произвольных неповторяющихся последовательностей;

б) система защиты по цепям питания, обеспечивающая невозможность функционирования специальных АС СКЗИ при нахождении питающих напряжений в недопустимых пределах;

в) система защиты по цепям питания, осуществляющая аппаратное или программное выравнивание/зашумление профиля энергопотребления;

г) система поиска ошибок, реализующая функции выявления несанкционированных изменений данных в памяти;

д) модуль защиты памяти (MPU) в части разграничения прав доступа к различным областям памяти со стороны пользователей и приложений;

е) датчик света, противодействующий оптическим атакам на критические цифровые узлы схемы;

ж) внутренний тактовый генератор с переменной частотой тактирования произвольным рандомизированным образом (без предъявлений требований к закону распределения, в диапазоне частот не хуже fтакт ±5%);

з) система защиты от утечки по ТКУИ.

Для аппаратных модулей безопасности информационной инфраструктуры платежных систем (HSM) и терминалов/банкоматов должны быть реализованы следующие меры защиты, входящие в АС СКЗИ[8]:

а) распределенный датчик объема, регистрирующий любое проникновение в корпус изделия;

б) датчик вскрытия корпуса;

в) модуль уничтожения ключевой информации в случае регистрации НСД.

В случае обнаружения попытки проникновения должно быть обеспечено доверенное уничтожение ключевой информации терминала. Такие защитные меры должны быть реализованы в АС СКЗИ.

Критичные функции или данные должны использоваться только в защищенной (ных) области(ях) устройства.

Для всех видов устройств в случае наличия обоснования обеспечения защиты от конкретной угрозы инженерного проникновения реализованными в СКЗИ мерами и средствами, отдельные аппаратные системы защиты, перечисленные выше, по согласованию с ФСБ России могут быть исключены.

---

[8] Для некоторых видов терминалов такие меры могут быть признаны избыточными по согласованию с ФСБ России.

5.6. Дополнительные требования по безопасности конфиденциальных данных в терминалах

Устройство не должно отображать введенные цифры ПИН-кода. Массив символов, показывающий ввод ПИН-кода, должен отображать только незначимые символы, например, звездочки.

Конфиденциальные данные не должны храниться дольше или использоваться чаще, чем это необходимо. ПИН-коды должны зашифровываться внутри устройства сразу после завершения ввода ПИН-кода. Устройство должно автоматически очищать свои внутренние буферы, когда транзакция завершена или истекло время ожидания устройством ответа от владельца карты или продавца.

Должно быть введено ограничение на количество действий, которые могут быть выполнены, и наложен лимит времени, после которого устройство вынуждено вернуться в нормальный режим.

Устройство должно обеспечить использование различных значений для ключей данных, ключей шифрования ключей и ключей шифрования ПИН.

В устройстве должен отсутствовать механизм, который позволял бы выводить симметричный или закрытый ключ или ПИН-код в открытом виде, шифровать такой ключ или ПИН-код ключом, который может быть известен нарушителю, или передавать такой ключ в открытом виде из одного компонента в другой.

Ввод любых других данных транзакции должен осуществляться отдельно от процесса ввода ПИН-кода, чтобы избежать случайного отображения ПИН-кода владельца карты на дисплее устройства. Если другие данные и ПИН-код вводятся на одной и той же клавиатуре, другой ввод данных и ввод ПИН-кода должны быть явно отдельными операциями.

Защита ПИН-кода во время передачи между устройством, зашифровавшим ПИН-код, и считывателем ICC должна быть реализована одним из следующих способов:

а) Если устройство, шифрующее ПИН-код, и считыватель ICC (карты) не интегрированы в один и тот же защищенный модуль, то метод проверки владельца карты определяется следующим образом:

- Зашифрованный ПИН-код: при передаче между устройством, зашифровавшим ПИН-код, и считывателем ICC ПИН-блок должен быть зашифрован с использованием либо ключа шифрования карты, либо с использованием ключа СКЗИ в терминале.
- Открытый ПИН-код: при передаче с устройства, зашифровавшего ПИН-код, на считыватель ICC (считыватель ICC затем расшифрует ПИН-код для передачи в виде открытого текста на карту) ICC ПИН-блок должен быть зашифрован с использованием ключа СКЗИ в терминале.

б) Если устройство, шифрующее ПИН-код, и считыватель ICC интегрированы в один и тот же защищенный модуль, и метод проверки владельца карты определяется следующим образом:

- Зашифрованный ПИН-код: ПИН-блок должен быть зашифрован с использованием ключа шифрования карты.

в) Открытый текст ПИН: шифрование не требуется, если блок ПИН передается полностью через защищенную среду (как определено в ISO 9564). Если открытый ПИН-код передается на считыватель ICC (платежной карты) через незащищенную среду, ПИН-блок должен быть зашифрован в соответствии с ISO 9564.

Панель ввода ПИН-кода (область ввода ПИН-кода) и окружающая область должны быть спроектированы таким образом, чтобы устройство затрудняло размещение мошеннического устройства поверх панели ПИН-кода.

5.7. Дополнительные требования по безопасности конфиденциальных данных в HSM

СКЗИ в HSM должны гарантировать использование разных ключей для разных криптографических функций. Например, недопустимо использование ключа шифрования ключа для шифрования ПИН-кода.

СКЗИ в HSM не должны содержать механизма, позволяющего выводить закрытые или симметричные ключи в открытом виде, а также шифрование ключа или ПИН-кода с использованием ключа, помеченного как скомпрометированный.

В должна быть исключена возможность ввода ПИН-кода в открытом виде. Управление ПИН-кодами СКЗИ HSM должно производиться в соответствии с требованиями рекомендаций по стандартизации Росстандарта или международных стандартов.

5.8. Положения по защите от ТКУИ

Принятые в технических средствах информационной инфраструктуры платежной системы меры защиты должны исключать возможность определения PIN и ключей шифрования, а также другой конфиденциальной информации путем анализа сигналов ТКУИ.

5.9. Положения по обновлению ПО СФ СКЗИ

Технические средства информационной инфраструктуры платежной системы могут предусматривать возможность обновления программного обеспечения СФ СКЗИ по каналам управления с аутентификацией субъекта, проводящего обновление, и технического средства информационной инфраструктуры платежной системы. Если аутентификация не подтверждается, то обновление производиться не должно.

От Банка России
Директор Департамента информационной безопасности
В.А. Уваров

От ФСБ России
Первый заместитель начальника Управления «А» 8 Центра ФСБ России
М.В. Федоров

Зам. начальника подразделения 8 Центра ФСБ России
В.М. Простов

Первый заместитель начальника 8 Центра ФСБ России
А.М. Шойтов

149/3/2/1-2945

А.М. Сычев

Васильев С.Н.

Начальник подразделения 8 Центра ФСБ России
Д.В. Матюхин