АО «СИГНАЛ-КОМ»

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «Крипто-КОМ 3.5»

ПОДСИСТЕМА УПРАВЛЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИЕЙ

Общее описание

ШКНР.00064-01 31 01

Листов 18

2022

Аннотация

В настоящем документе рассматриваются вопросы управления ключевой системой, используемой в СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2), с учетом мер, обеспечивающих безопасность использования ключей электронной подписи и ключевого обмена.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2), должны разрабатываться с учетом требований настоящего документа.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) предназначено для криптографической защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в информационных системах общего пользования.

Ключевая система СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) ориентирована на совместное использование одноключевых и двухключевых криптосистем.

2. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ И ХАРАКТЕРИСТИКИ

СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) удовлетворяет «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по уровню КС1, а при выполнении дополнительных требований по защите от несанкционированного доступа – по уровню КС2 [11]. Допускается использование СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) для криптографической защиты персональных данных.

2.1. Криптографические алгоритмы

СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) включает реализацию следующих алгоритмов:

- алгоритмы создания ЭП, ключей ЭП и ключей проверки ЭП - реализованы в соответствии с требованиями ГОСТ Р 34.10-2012 [4];
- алгоритмы проверки ЭП - реализованы в соответствии с требованиями ГОСТ Р 34.10-2001 [3] и ГОСТ Р 34.10-2012 [4];
- алгоритмы выработки значения хэш-функции - реализованы в соответствии с требованиями ГОСТ Р 34.11-94 [5] и ГОСТ Р 34.11-2012 [6];
- алгоритмы зашифрования/расшифрования данных и вычисления имитовставки - реализованы в соответствии с требованиями ГОСТ 28147-89 [2], ГОСТ Р 34.12-2015 [7], ГОСТ Р 34.13-2015 [8];
- алгоритмы согласования ключей - реализованы в соответствии с Рекомендациями по стандартизации Р 50.1.113-2016 [9].

Использование реализованных в СКЗИ криптографических механизмов, определяемых выведенным из действия стандартом ГОСТ 28147-89, после 30.06.2024 запрещается.

Ключевая система СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) ориентирована на совместное использование одноключевых и двухключевых криптосистем.

2.1.1. Реализация ГОСТ 28147-89

Включение в СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) реализации зашифрования, расшифрования и вычисления имитовставки в соответствии с ГОСТ 28147-89 обусловлено необходимостью обеспечения совместимости с СКЗИ, реализующими ГОСТ 28147-89 и имеющими действующие сертификаты соответствия ФСБ России. При этом использование реализованных в СКЗИ криптографических механизмов, определяемых выведенным из действия стандартом ГОСТ 28147-89, после 30.06.2024 запрещается.

В СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) используются следующие режимы криптографического преобразования в соответствии с ГОСТ 28147-89 [2]:

- зашифрование/расшифрование в режиме простой замены;
- зашифрование/расшифрование в режиме гаммирования;
- зашифрование/расшифрование в режиме гаммирования с обратной связью;
- выработка имитовставки.

При зашифровании/расшифровании и выработке имитовставки используется алгоритм преобразования ключа, описанный в п. 2.3.2 RFC 4357 [19].

Для зашифрования и расшифрования информации ГОСТ 28147-89 предусматривает использование одного и того же ключа криптопреобразования (общий секретный ключ связи) длиной 256 бит и узлов замены (блока подстановки) общим объемом в 512 бит, содержимое которых является долговременным ключевым элементом, общим для защищаемой сети конфиденциальной связи.

2.1.2. Реализация ГОСТ Р 34.12-2015

В СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) реализованы алгоритмы блочного шифрования Кузнечик и Магма в соответствии с ГОСТ Р 34.12-2015 [7].

В СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) используются следующие режимы криптографического преобразования в соответствии с ГОСТ Р 34.13-2015 [8], а также рекомендациями по стандартизации [10, 12]:

- зашифрование/расшифрование в режиме простой замены;

- зашифрование/расшифрование в режиме простой замены с зацеплением;
- зашифрование/расшифрование в режиме гаммирования;
- зашифрование/расшифрование в режиме гаммирования с обратной связью по выходу;
- зашифрование/расшифрование в режиме гаммирования с обратной связью по шифртексту;
- зашифрование/расшифрование в режиме CTR-ACPKM согласно [10];
- зашифрование/расшифрование в режиме MGM согласно [12];
- выработка имитовставки – OMAC согласно [8].
- выработка имитовставки – OMAC-ACPKM согласно [10].

Для зашифрования и расшифрования информации ГОСТ Р 34.12-2015 предусматривает использование одного и того же ключа криптопреобразования (общий секретный ключ связи) длиной 256 бит.

2.1.3. Реализация ГОСТ Р 34.11-94

ГОСТ Р 34.11-94 [5] определяет алгоритм и процедуру вычисления хэш-функции для любой последовательности двоичных символов, которые применяются в криптографических методах обработки и защиты информации, в том числе и для реализации процедур электронной подписи.

Определенная в ГОСТ Р 34.11-94 функция хэширования используется при реализации систем ЭП на базе асимметричных криптографических алгоритмов в соответствии с ГОСТ Р 34.10-2001.

2.1.4. Реализация ГОСТ Р 34.11-2012

ГОСТ Р 34.11-2012 [6] определяет алгоритм и процедуру вычисления хэш-функции для любой последовательности двоичных символов, которые применяются в криптографических методах обработки и защиты информации, в том числе и для реализации процедур электронной подписи.

Определенная в ГОСТ Р 34.11-2012 функция хэширования используется при реализации систем ЭП на базе асимметричных криптографических алгоритмов в соответствии с ГОСТ Р 34.10-2012.

2.1.5. Реализация ГОСТ Р 34.10-2001

ГОСТ Р 34.10-2001 [3] устанавливает процедуры создания и проверки ЭП, реализуемой с использованием операций группы точек эллиптической кривой, определенной над конечным простым полем.

Стойкость ЭП, формируемой в соответствии с ГОСТ Р 34.10-2001, основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также стойкости используемой хэш-функции по ГОСТ Р 34.11-94.

Электронная подпись состоит из двух целых чисел и вычисляется с помощью набора правил, задаваемых стандартом ГОСТ Р 34.10-2001.

Параметры системы ЭП не являются секретными, конкретный набор их значений может быть общим для группы пользователей.

В СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) реализован только алгоритм проверки ЭП в соответствии с ГОСТ Р 34.10-2001.

2.1.6. Реализация ГОСТ Р 34.10-2012

ГОСТ Р 34.10-2012 [4] устанавливает процедуры создания и проверки ЭП, реализуемой с использованием операций группы точек эллиптической кривой, определенной над конечным простым полем.

Стойкость ЭП, формируемой в соответствии с ГОСТ Р 34.10-2012, основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также стойкости используемой хэш-функции по ГОСТ Р 34.11-2012 [6].

Электронная подпись состоит из двух целых чисел и вычисляется с помощью набора правил, задаваемых стандартом ГОСТ Р 34.10-2012.

Параметры системы ЭП не являются секретными, конкретный набор их значений может быть общим для группы пользователей.

2.2. Ключевые носители

Криптографические ключи и вспомогательные данные (маски и т.п.), используемые в СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2), будем называть *ключевой информацией*[1], а магнитные носители и другие внешние устройства, на которые записываются ключи при создании - *ключевыми носителями*.

Для хранения ключевой информации в СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) могут быть использованы следующие типы ключевых носителей (см. Таблица 1):

Таблица 1

Тип ключевого носителя	Уровень защиты
Носители с интерфейсом USB	КС1, КС2
Электронные ключи с интерфейсом USB (eToken, JaCarta, Rutoken и др.)	КС1, КС2
Криптографические устройства, перечисленные в п. 2.3	КС1, КС2
Карты флэш-памяти	КС1, КС2
Разделы накопителей на жестком магнитном диске (НЖМД)	КС1, КС2

Примечание. Хранение ключей ЭП в разделе жесткого диска допускается только при условии распространения на ЭВМ (или съемный НЖМД ЭВМ) требований по обращению с ключевыми носителями.

2.3. Ключевые носители с неэкспортируемыми ключами

СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) может обращаться через интерфейс PKCS#11 к криптографическим устройствам, реализующим функции создания ключей ЭП и ключей проверки ЭП, создания ЭП, проверки ЭП, хэширования, шифрования, ключевого обмена, выработки случайных последовательностей и др. Данные устройства могут также использоваться для хранения ключей ЭП в неэкспортируемом виде, исключающем возможность их считывания во внешнюю память или копирование на другой носитель.

СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) может использовать механизмы (создания ключей ЭП и ключей проверки ЭП, создание ЭП, проверка ЭП, хэширование, шифрование, ключевой обмен, выработка случайных последовательностей и др.), реализованные в криптографических устройствах, совместно с программной реализацией криптографических алгоритмов СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) (хэширование, шифрование и др.).

Перечень криптографических устройств с интерфейсом PKCS #11, поддерживаемых СКЗИ «Крипто-КОМ 3.5» (вариант исполнения 1), включает[2]:

- СКЗИ «SmartToken-PRO»;
- СКЗИ «Рутокен ЭЦП 2.0 2100» (сертификат соответствия № СФ/124-4248 от 10.04.2022);
- СКЗИ «Рутокен ЭЦП 2.0 3000» (сертификат соответствия № СФ/124-4077 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 3000 micro» (сертификат соответствия № СФ/124-4078 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 3000 Type-C» (сертификат соответствия № СФ/124-4079 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 Flash» (сертификат соответствия № СФ/121-4075 от 17.06.2021);

[1] Создание ключевой информации должно выполняться с помощью специализированного программного обеспечения, разработанного с использованием СКЗИ, сертифицированного ФСБ России.

[2] Криптографические устройства должны иметь действующий сертификат соответствия (заключение о соответствии) ФСБ России.

- СКЗИ «Рутокен ЭЦП 2.0 micro» (сертификат соответствия № СФ/124-3991 от 11.12.2020);
- СКЗИ «Рутокен ЭЦП 2.0» (сертификат соответствия № СФ/124-3990 от 02.12.2020);
- СКЗИ «Рутокен ЭЦП 2.0 Исполнение А» (сертификат соответствия № СФ/121-4072 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 Touch» (сертификат соответствия № СФ/124-3993 от 11.12.2020);
- СКЗИ «Рутокен ЭЦП 3.0» (варианты исполнения 1, 2) (сертификат соответствия № СФ/124-4307 от 11.08.2022);
- СКЗИ «Рутокен ЭЦП 3.0» (вариант исполнения 5) (сертификат соответствия № СФ/124-4398 от 01.12.2022);
- СКЗИ «MS_KEY K» – «АНГАРА» (вариант исполнения 8.1.1) (сертификат соответствия № СФ/124-4311 от 12.08.2022);
- СКЗИ «ESMART Token ГОСТ на базе отечественной микросхемы MIK51SC72DV6» (варианты исполнения 1, 2, 3) (сертификат соответствия № СФ/124-4048 от 01.04.2021).

Перечень криптографических устройств с интерфейсом PKCS #11, поддерживаемых СКЗИ «Крипто-КОМ 3.5» (вариант исполнения 2), включает:

- СКЗИ «Рутокен ЭЦП 2.0 2100» (сертификат соответствия № СФ/124-4248 от 10.04.2022);
- СКЗИ «Рутокен ЭЦП 2.0 3000» (сертификат соответствия № СФ/124-4077 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 3000 micro» (сертификат соответствия № СФ/124-4078 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 3000 Type-C» (сертификат соответствия № СФ/124-4079 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 Flash» (сертификат соответствия № СФ/121-4075 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 micro» (сертификат соответствия № СФ/124-3991 от 11.12.2020);
- СКЗИ «Рутокен ЭЦП 2.0» (сертификат соответствия № СФ/124-3990 от 02.12.2020);
- СКЗИ «Рутокен ЭЦП 2.0 Исполнение А» (сертификат соответствия № СФ/121-4072 от 17.06.2021);
- СКЗИ «Рутокен ЭЦП 2.0 Touch» (сертификат соответствия № СФ/124-3993 от 11.12.2020);
- СКЗИ «Рутокен ЭЦП 3.0» (варианты исполнения 1, 2) (сертификат соответствия № СФ/124-4307 от 11.08.2022);
- СКЗИ «Рутокен ЭЦП 3.0» (вариант исполнения 5) (сертификат соответствия № СФ/124-4398 от 01.12.2022);
- СКЗИ «MS_KEY K» – «АНГАРА» (вариант исполнения 8.1.1) (сертификат соответствия № СФ/124-4311 от 12.08.2022).;
- СКЗИ «ESMART Token ГОСТ на базе отечественной микросхемы MIK51SC72DV6» (варианты исполнения 2, 3) (сертификат соответствия № СФ/124-4048 от 01.04.2021).

3. ОБЩЕЕ ОПИСАНИЕ КЛЮЧЕВОЙ СИСТЕМЫ

Ключевая система СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) ориентирована на совместное использование одноключевых и двухключевых криптосистем.

В системах защиты информации, построенных на базе СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2), ключи проверки ЭП пользователей используются, хранятся и передаются по каналам связи в виде цифровых сертификатов ключей проверки ЭП (см. п.3.1.3), которые формируются и заверяются в удостоверяющем центре (см.п. 4.1).

Удостоверяющий центр (УЦ) в лице главного администратора безопасности УЦ (далее – администратор безопасности) отвечает за администрирование подсистемы управления ключами проверки ЭП, обеспечивающей контроль за выполнением всех процедур, связанных с созданием, регистрацией, хранением и обновлением ключевых носителей участников защищенной системы.

Управление ключами проверки ЭП СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) может обеспечиваться любым УЦ, сертифицированным ФСБ России по «Требованиям к средствам удостоверяющего центра» (приложение к Приказу ФСБ Российской Федерации № 796 от 27.12.2011) и создающим сертификаты ключей проверки ЭП и списки аннулированных сертификатов ключей проверки ЭП (CAC) в соответствии с Рекомендациями ITU-T X.509 [17] (далее - X.509) и IETF RFC 5280 [18], Рекомендациями по стандартизации Р 1323565.1.023-2018 [11].

В зависимости от требований политики безопасности эксплуатирующей организации, СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) допускает возможность создания ключей ЭП и ключей проверки ЭП пользователей как децентрализовано - самостоятельно самими пользователями на своих рабочих местах, так и централизовано – администратором безопасности.

3.1. Ключевая информация

3.1.1. Симметричные ключи шифрования

В СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) для симметричных криптопреобразований используются одноключевые алгоритмы шифрования с длиной ключа 256 бит, выполненные в соответствии с требованиями ГОСТ 28147-89 [2], ГОСТ Р 34.12-2015 [7], ГОСТ Р 34.13-2015 [8] и реализующие различные режимы:

- простой замены;
- гаммирования;
- гаммирования с обратной связью;
- выработки имитовставки.

Режим простой замены должен использоваться только для зашифрования/расшифрования криптографических ключей, режимы гаммирования и гаммирования с обратной связью - для зашифрования/расшифрования информации, режим выработки имитовставки - для подтверждения целостности информации.

Подсистема управления ключевой информации СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) использует динамическое создание симметричных ключей шифрования. При динамическом создании симметричные ключи формируются по мере необходимости приложениями, построенными на базе СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2), с использованием методов открытого распределения ключей.

Использование реализованных в СКЗИ криптографических механизмов, определяемых выведенным из действия стандартом ГОСТ 28147-89, после 30.06.2024 запрещается.

3.1.2. Ключи электронной подписи и ключевого обмена

СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) поддерживает криптосистемы с открытым распределением ключей, предполагающие наличие у каждого пользователя пары ключей - закрытого и открытого.

В приложениях на базе СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2), использующих асимметричные криптосистемы, закрытый ключ может применяться как для создания электронной подписи, так и при ключевом обмене. Использование закрытого ключа в качестве ключа ЭП и/или ключевого обмена определяется сведениями, указанными в сертификате соответствующего открытого ключа (см. п. 3.1.3).

3.1.2.1. Ключи ключевого обмена

В СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) для зашифрования и расшифрования информации используется общий секретный ключ связи. Создание общего секретного ключа связи для шифрования информации выполняется с использованием закрытого ключа ключевого обмена отправителя и открытого ключа ключевого обмена получателя, а для расшифрования информации - с использованием закрытого ключа ключевого обмена получателя и открытого ключа ключевого обмена отправителя. При этом закрытый и открытый ключи ключевого обмена могут быть временными (одноразовыми).

3.1.2.2. Ключи электронной подписи

В СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) для создания электроной подписи реализованы двухключевые алгоритмы, выполненные в соответствии с требованиями ГОСТ Р 34.10-2001 [3], ГОСТ Р 34.10-2012 [4], а также алгоритмы вычисления функции хэширования, выполненные в соответствии с требованиями ГОСТ Р 34.11-94 [5], ГОСТ Р 34.11-2012 [6].

При создании электронной подписи используется ключ ЭП пользователя, а при проверке подписи – его ключ проверки ЭП. В процессе создания ЭП исходное сообщение произвольного объема преобразуется в хэш-значение длиной 256 или 512 бит.

3.1.3. Сертификаты ключей проверки ЭП и списки аннулированных сертификатов

В асимметричных криптосистемах, построенных на базе СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2), ключ проверки ЭП можно использовать только при условии достоверного подтверждения его подлинности (отсутствие искажений и принадлежность определенному лицу), что обеспечивается заверением ключа проверки ЭП третьей доверенной стороной (использование ключа проверки ЭП в составе цифрового сертификата, заверенного удостоверяющим центром, или нотариальное заверение копии ключа проверки ЭП на бумажном носителе, собственноручно подписанном владельцем ключа).

Цифровым сертификатом ключа проверки ЭП называется структурированный двоичный набор данных в формате, определенном Рекомендациями ITU-T X.509 [17], включающий следующую информацию:

- уникальный серийный номер сертификата;
- идентификатор алгоритма, используемого для ЭП;
- уникальное имя издателя сертификата;
- даты начала и окончания срока действия сертификата;
- имя пользователя или объекта системы, однозначно идентифицирующего его в рамках данной системы;
- информацию о ключе проверки ЭП пользователя или объекте системы: идентификатор алгоритма и собственно ключ проверки ЭП;
- дополнительные атрибуты (расширения) сертификата, определяющие назначение ключа в соответствии с требованиями его использования в системе;
- ЭП издателя сертификата (уполномоченного лица УЦ).

Сертификатом ключа проверки электронной подписи в терминологии № 63-ФЗ «Об электронной подписи» называется электронный документ или документ на бумажном носителе, выданный УЦ либо доверенным лицом УЦ и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП [1].

В СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) сертификатом может служить цифровой сертификат ключа проверки ЭП в формате X.509, а также учетная карточка, представляющая собой бумажный бланк, на котором распечатаны ключ проверки ЭП и реквизиты пользователя, заверенные печатью и подписью уполномоченного лица УЦ (администратора или администратора безопасности).

Ключи проверки ЭП пользователей передаются на регистрацию и последующую сертификацию в УЦ в составе запроса на создание сертификата ключа проверки ЭП. Запросы на создание сертификата ключа проверки ЭП могут формироваться приложениями, построенными на базе СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2).

При работе с ключами проверки ЭП пользователю необходимо иметь справочник ключей проверки ЭП других пользователей. Доведение до пользователей и обновление данных справочников является задачей администратора безопасности.

При регистрации нового пользователя или при выводе из действия ранее зарегистрированных ключей, все пользователи сети конфиденциальной связи должны обновлять свои локальные справочники ключей проверки ЭП.

Регламент работы со справочниками ключей проверки ЭП определяется организацией, эксплуатирующей СКЗИ, и закрепляется либо в виде отдельного документа, либо входит в состав должностной инструкции администратора безопасности. При создании подобного регламента необходимо учитывать следующие рекомендации:

- справочник ключей проверки ЭП требует периодического обновления по мере изменения или добавления ключей в данном справочнике; обновление справочников может быть построено либо по принципу принудительной рассылки, либо по принципу опубликования в общедоступных источниках (например, через LDAP сервер);
- при использовании в прикладном программном обеспечении криптографических функций необходимо обеспечить контроль актуальности справочника на данный момент времени;
- при обновлении справочников ключей проверки ЭП старые справочники с ключами проверки ЭП необходимо сохранять в архиве для последующих процедур разбора конфликтных ситуаций (см. п. 4.2);
- чтобы исключить подделку справочника сертификатов ключей проверки ЭП, при каждом использовании сертификата ключа проверки ЭП должна выполняться проверка ЭП УЦ под сертификатом ключа проверки ЭП.

УЦ может аннулировать (заблокировать) выданный им сертификат ключа проверки ЭП (например, в случае компрометации соответствующего ключа ЭП). Для доведения до пользователей информации об аннулированных сертификатах ключей проверки ЭП УЦ выпускает списки аннулированных сертификатов ключей проверки ЭП (CAC), заверенные электронной подписью УЦ и включающие в себя перечень серийных номеров сертификатов ключей проверки ЭП, аннулированных на определенный момент времени.

Чтобы исключить возможность использования скомпрометированного или аннулированного сертификата ключа проверки ЭП, наряду с проверкой ЭП УЦ под сертификатом ключа проверки ЭП должен выполняться поиск ссылки на данный сертификат в списке аннулированных сертификатов ключей проверки ЭП и проверка ЭП УЦ под списком.

3.2. Ключевая система

3.2.1. Структура ключевого хранилища

В «Крипто-КОМ 3.5» (варианты исполнения 1, 2) реализована концепция хранилища (или контейнера) ключей и дополнительной служебной информации, предусматривающая их хранение либо в зашифрованном, либо в замаскированном виде.

В контейнер включаются:

- главный ключ;
- маски главного ключа;
- ключ шифрования ключей (key encryption key - KEK); зашифрован на главном ключе;
- вектор состояния (инициализирующая последовательность) для программного датчика случайных чисел (может отсутствовать, см. п. 3.2.2); зашифрован на KEK;
- произвольное количество ключей электронной подписи и ключевого обмена, зашифрованных на KEK.

В хранилище реализован механизм контроля целостности объектов с использованием имитовставки.

СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) предусматривает хранение главного ключа и вектора состояния программного датчика случайных чисел (если он используется) в файлах, располагаемых на одном из носителей, перечисленных в п.2.2.

Способ хранения других объектов ключевой системы не оговаривается.

Маски главного ключа рекомендуется хранить отдельно от главного ключа (на другом носителе).

Одновременно может использоваться произвольное число контейнеров (хранилищ).

Приложения, построенные на базе СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) могут использовать дополнительные методы защиты ключевой информации (например,

парольную защиту либо организационно-техническое разделение ключа на несколько частей [21]).

3.2.2. Создание ключевой информации

В СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) ключи ЭП и ключи ключевого обмена формируются с помощью аппаратного или программного датчика случайных чисел.

В качестве источника аппаратно-генерируемых случайных чисел могут использоваться физические ДСЧ следующих программно-аппаратных средств защиты информации, при наличии действующего сертификата ФСБ России[1]:

- ПАК защиты от НСД «Соболь» (версии кода расширения BIOS 1.0.99, 1.0.180);
- СЗИ НСД «Аккорд-АМДЗ» (версия 3.2);
- АПМДЗ «Криптон-ЗАМОК/К» (изделие М-526А);
- АПМДЗ «Криптон-ЗАМОК/У» (изделие М-526Б).

Источники аппаратно-генерируемых случайных чисел могут использоваться только при наличии действующего сертификата ФСБ России.

Функция выработки случайных чисел автоматически определяет наличие одного из перечисленных устройств и устанавливает соответствующий метод выработки случайных чисел.

Программный датчик случайных чисел (ПДСЧ) строится на основе ГОСТ Р 34.12-2015 (алгоритм блочного шифрования «Кузнечик») [7] в режиме CTR-ACPKM [10] и может быть инициализирован:

- от физического датчика случайных чисел перечисленных выше программно-аппаратных средств защиты информации;
- от БДСЧ, входящего в состав СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2);
- от вектора состояния (инициализирующей последовательности) ПДСЧ, сохраненного в контексте ключевого контейнера.

При инициализации биологического ДСЧ пользователю предлагается совершать нажатия (поддерживаемыми методами ввода, такими как манипулятор «мышь», сенсорный экран) в произвольном порядке на изображения кругов в новом окне ОС на дисплее. После каждого нажатия по кругу производится выработка бинарной информации из энтропии случайных действий пользователя, эта информация накапливается с каждым нажатием. В процессе инициализации производится оперативный статистический контроль качества накопленной бинарной информации и автоматически определяется достаточность количества нажатий. При достижении достаточного количества нажатий накопленная бинарная информация обрабатываются с помощью функции хэширования по ГОСТ Р 34.11-2012 (256 бит). Результатом работы алгоритма является результат функции хэширования - массив случайных данных размером 256 бит, который используется для инициализации программного датчика случайных чисел.

Вектор состояния (инициализирующая последовательность) ПДСЧ может быть сохранен в зашифрованном виде, в контексте ключевого контейнера (см. п. 3.2.1) и позднее использован при последующей инициализации ПДСЧ.

Повторное использование вектора состояния ПДСЧ недопустимо, поэтому вектор состояния должен уничтожаться сразу после считывания с носителя, на котором он был сохранен. По этой же причине при создании резервных копий ключевых носителей не допускается копирование вектора состояния.

В качестве источника случайных чисел могут использоваться также, криптографические устройства, перечисленные в п. 2.3. Выбор способа создания ключей при работе с СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) определяется регламентом работы сети конфиденциальной связи и требованиями к уровню защищенности СКЗИ (КС1 или КС2), установленного на рабочем месте владельца ключей.

В СКЗИ всех классов могут использоваться как физические, так и программные ДСЧ.

Подсистема управления ключевой информацией СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) допускает несколько способов создания ключей ЭП и ключей проверки ЭП пользователей, отличающихся

[1] Перечень источников аппаратно-генерируемых случайных чисел может изменяться и расширяться.

режимом создания:

- централизованный - ключи пользователей создаются администратором безопасности и затем передаются пользователям;
- децентрализованный – пользователи самостоятельно создают ключи на своих рабочих местах;

типом ДСЧ, используемого при создании ключей:

- физический ДСЧ одного из ПАК защиты от НСД, сертифицированных ФСБ России;
- программный ДСЧ из состава СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2);
- ДСЧ криптографических устройств, перечисленных в п. 2.3.

В подсистеме управления ключевой информацией СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2), созданные ключи проверки ЭП пользователей передаются на сертификацию в УЦ (см. п. 4.1).

3.3. Требования к ключевым носителям

Перед записью на ключевой носитель ключевой информации ключевой носитель должен быть отформатирован.

Ключи ЭП пользователя относятся к конфиденциальной информации. Пользователь должен обеспечить надежное хранение в тайне своего ключа ЭП.

Пользователь несет персональную ответственность за хранение личных ключевых носителей.

При хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям лиц, не назначенных для работы с конкретным ключевым носителем.

Запрещается оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации

При централизованном хранении ключевых носителей участников защищенной системы конфиденциальной связи на предприятии, эксплуатирующем СКЗИ, должны быть выделены специальные лица, ответственные за хранение:

- администратор безопасности;
- администратор безопасности группы пользователей (администратор группы).

Администратор безопасности группы пользователей может назначаться при значительном количестве пользователей в подразделениях предприятия для более удобной организации управления ключевой системой на местах. Администратору группы делегируются права регистрации пользователей и их ключей у администратора безопасности (УЦ).

При централизованном хранении ключей администраторы группы и администратор безопасности несут персональную ответственность за хранение личных ключевых носителей пользователей.

Факт выдачи ключевых носителей пользователю фиксируется администратором безопасности в «Журнале учета и движения ключевых носителей».

При хранении ключей ЭП в разделе жесткого диска ПЭВМ или в реестре ОС Windows рекомендуется использовать парольную защиту.

При хранении ключей в реестре ОС Windows или в разделе жесткого диска ЭВМ требования по хранению личных ключевых носителей распространяются на ЭВМ (НЖМД ЭВМ).

В случае невозможности отчуждения ключевого носителя с ключевой информацией от ЭВМ, организационно-техническими мероприятиями должен быть исключен доступ нарушителей к ЭВМ с ключами.

В случае необходимости проведения ремонтных и регламентных работ аппаратной части СКЗИ или среды функционирования (СФ) необходимо обеспечить невозможность доступа нарушителя к ключевой информации, содержащейся в аппаратной части СКЗИ/СФ. Конкретный перечень мер должен быть определен, исходя из условий эксплуатации СКЗИ.

3.4. Длина ключей

В СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) допустимо использование ключей следующей длины:

- длина ключей ЭП по ГОСТ Р 34.10-2012 – 256 или 512 бит;

- длина ключей проверки ЭП по ГОСТ Р 34.10-2012 – 512 или 1024 бит;
- длина ключей проверки ЭП по ГОСТ Р 34.10-2001 – 512 бит;
- длина закрытых ключей ключевого обмена на эллиптических кривых – 256 или 512 бит;
- длина открытых ключей ключевого обмена на эллиптических кривых – 512 или 1024 бит;
- длина ключей шифрования и выработки имитовставки по ГОСТ 28147-89 – 256 бит;
- длина ключей шифрования и выработки имитовставки по ГОСТ Р 34.12-2015 – 256 бит.

Использование реализованных в СКЗИ криптографических механизмов, определяемых выведенным из действия стандартом ГОСТ 28147-89, после 30.06.2024 запрещается.

3.4.1. Сроки действия ключей

В СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) допускаются следующие сроки действия ключей:

- максимальный срок действия ключа ЭП – 1 год 3 месяца;
- максимальный срок действия ключа проверки ЭП (сертификата ключа проверки ЭП) – не должен превышать срока действия соответствующего ключа ЭП более чем на 15 лет.

Возможность увеличения срока действия ключей ЭП может быть рассмотрена при условии обеспечения дополнительных организационно-технических мер защиты, исходя из конкретных условий эксплуатации, в процессе проведения тематических исследований СКЗИ, построенного на базе СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2).

При использовании в качестве ключевых носителей криптографических устройств из состава СКЗИ, обеспечивающих хранение ключей ЭП в неэкспортируемом виде (см. п. 2.3), максимальный срок действия ключей определяется эксплуатационной документацией на данные устройства.

3.4.2. Уничтожение ключевых носителей

Ключи ЭП, выведенные из действия в результате завершения их срока действия, при досрочном обновлении или компрометации, должны быть уничтожены пользователями и администраторами безопасности со всех ключевых носителей (дискет, USB-токены и др.).

Для уничтожения ключей с ключевых носителей используется утилита wipe из состава СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2), предназначенная для удаления файлов с ключевых носителей с предварительным их физическим затиранием. Порядок использования утилиты приводится в документе [16].

USB-токены и другие ключевые носители должны быть отформатированы и в дальнейшем могут быть повторно использованы только в качестве носителей ключевой информации.

Факт уничтожения ключей фиксируется в «Журнале учета и движения ключевых носителей».

Для разрешения конфликтных ситуаций, связанных с применением ЭП, ключи проверки ЭП должны сохраняться в архиве ключей проверки ЭП администратора безопасности в течение срока, определенного политикой безопасности организации.

4. РЕКОМЕНДАЦИИ ПО УПРАВЛЕНИЮ КЛЮЧЕВОЙ СИСТЕМОЙ

В настоящем разделе приводятся рекомендации по управлению ключевой системой, организованной на базе удостоверяющего центра (УЦ).

4.1. Удостоверяющий центр

В сетях конфиденциальной связи, создаваемых на базе СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2), УЦ представляет собой организационно-административную структуру, отвечающую за проведение политики информационной безопасности.

Использование УЦ обеспечивает выполнение всех необходимых процедур администрирования, связанных с созданием, регистрацией, хранением, обновлением и распространением ключей проверки ЭП и ключевых носителей всех участников защищенной сети конфиденциальной связи.

УЦ подсистемы управления ключевой информацией должен обеспечивать выполнение следующих базовых функций, которые должны поддерживаться в соответствии с положениями Федерального закона № 63-ФЗ «Об электронной подписи» [1]:

- создание ключей ЭП и ключей проверки ЭП УЦ (уполномоченного лица УЦ);
- создание корневых (самоподписанных) сертификатов ключей проверки ЭП УЦ;
- создание и хранение рабочих и резервных ключевых носителей УЦ;
- регистрация пользователей сети конфиденциальной связи;
- создание и хранение рабочих и резервных ключевых носителей пользователей при централизованном управлении;
- прием и регистрация запросов на создание сертификатов ключей проверки ЭП пользователей;
- верификация запросов и контроль уникальности ключей проверки ЭП в регистрируемых запросах;
- создание сертификатов ключей проверки ЭП пользователей;
- выдача сертификатов ключей проверки ЭП пользователей в электронной форме и в форме документов на бумажных носителях;
- сохранение запросов на создание сертификата ключа проверки ЭП в течение установленного срока хранения;
- доставка сертификатов ключей проверки ЭП пользователям;
- приостановление и возобновление действия сертификатов ключей проверки ЭП, а также их аннулирование;
- изготовление списков аннулированных сертификатов ключей проверки ЭП пользователей (CAC);
- ведение реестра выпущенных сертификатов ключей проверки ЭП и списков аннулированных сертификатов ключей проверки ЭП;
- ведение журналов учета ключевых носителей (зарегистрированных, уничтоженных, хранящихся в УЦ и выданных пользователям);
- организация схемы оперативного оповещения пользователей обо всех изменениях в сети (компрометация ключей, восстановление конфиденциальной связи после компрометации ключей, включение новых пользователей, плановая смена ключей и т.п.);
- разбор конфликтных ситуаций, связанных с доказательством авторства электронного документа, снабженного электронной подписью и др.;
- проведение мероприятий по локализации и ликвидации последствий компрометации ключей.

Удостоверяющие центры, используемые в сетях конфиденциальной связи, создаваемых на базе СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) , должны быть сертифицированы по «Требованиям к средствам удостоверяющего центра» [11].

4.2. Порядок разбора конфликтных ситуаций, связанных с применением ЭП

Применение электронной подписи в сети конфиденциальной связи (далее – системы) может вызвать конфликтные ситуации, заключающиеся в оспаривании сторонами (участниками системы) авторства и/или содержимого документа, подписанного электронной подписью.

Разбор подобных конфликтных ситуаций в соответствии с действующим законодательством и особенностями создания самой электронной подписи требует применения специального программного обеспечения.

Разбор конфликтной ситуации заключается в доказательстве авторства подписи конкретного электронного документа конкретным исполнителем. Данный разбор основывается на математических свойствах алгоритма ЭП, реализованного в соответствии со стандартами Российской Федерации ГОСТ 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012, гарантирующих невозможность подделки значения ЭП любым лицом, не обладающим ключом электронной подписи.

При проверке значения ЭП используется ключ проверки ЭП, парный ключу ЭП, с помощью которого выполнялась процедура создания ЭП.

На случай разрешения споров в системе должно быть предусмотрено ведение архивов ключей проверки ЭП (сертификатов ключей проверки ЭП) и электронных документов с ЭП.

Для разбора конфликтной ситуации рекомендуется созывать комиссию, состоящую из представителей сторон, службы безопасности и экспертов (при необходимости).

Состав комиссии, порядок ее формирования, регламент работы, рассмотрение результатов ее работы определяется в приложении к Договору, заключаемому между участниками системы.

Оспаривание результатов работы комиссии и возмещение пострадавшей стороне принесенного ущерба выполняется в установленном действующим законодательством Российской Федерации порядке.

4.2.1. Порядок разбора конфликтной ситуации

Разбор конфликтной ситуации выполняется по инициативе любого участника системы и включает:

- предъявление претензии одной стороны другой;
- формирование комиссии;
- разбор конфликтной ситуации;
- взыскание с виновной стороны принесенного ущерба.

При разборе конфликтной ситуации, связанной с признанием авторства электронной подписи под спорным документом, используется программное обеспечение СКЗИ, сертифицированного ФСБ России.

В защищенных системах, использующих сертификаты ключей проверки ЭП, проверка подписанного электронного документа включает в себя выполнение следующих действий:

- определение сертификата ключа проверки ЭП или нескольких сертификатов ключей проверки ЭП, необходимых для проверки ЭП;
- проверка ЭП электронного документа с использованием каждого сертификата ключа проверки ЭП;
- проверка ЭП каждого сертификата ключа проверки ЭП, путем построения цепочки сертификатов ключей проверки ЭП до сертификата ключа проверки ЭП главного (корневого) УЦ;
- проверка действительности сертификатов ключей проверки ЭП на текущий момент времени;
- проверка действительности сертификатов ключей проверки ЭП на момент создания ЭП;
- проверка отсутствия сертификатов ключей проверки ЭП в САС.

Если сертификат ключа проверки ЭП, с использованием которого проверяется ЭП, аннулирован (т.е. включен в САС), комиссия принимает решение о действительности ЭП документа, используя дату создания документа и дату аннулирования сертификата ключа проверки ЭП в САС.

При проверке ЭП документа, верификации цепочки сертификатов ключей проверки ЭП, отсутствии сертификата ключа проверки ЭП в САС, составляется «Протокол проверки ЭП», в котором фиксируются сертификаты ключей проверки ЭП, использованные для проверки, и факт подтверждения или неподтверждения ЭП. Данный протокол является основным документом работы комиссии и должен быть подписан всеми ее членами.

В случае подтверждения электронной подписи, значения ключей проверки ЭП в составе сертификатов ключей проверки ЭП, указанных в протоколе проверки, необходимо сравнить со значениями ключей проверки ЭП соответствующих бумажных копий, заверенных администратором УЦ (см. п. 4.1). При совпадении их значений, авторство ЭП под документом считается установленным.

4.2.2. Случаи невозможности проверки значения ЭП

Доказать авторство документа, подписанного электронной подписью, не представляется возможным при отсутствии в архивах ключа проверки ЭП (сертификата ключа проверки ЭП) пользователя, выполнившего ЭП, или его бумажной копии, заверенной пользователем и администратором УЦ. В связи с этим, для архива с ключами проверки ЭП (сертификатами ключей проверки ЭП) необходимо периодически создавать резервные копии, а бумажные копии сертификатов ключей проверки ЭП должны храниться в течение всего установленного срока хранения.

ЛИТЕРАТУРА

1. Закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».
2. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
3. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной подписи.
4. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
5. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.
6. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.
7. ГОСТ Р 34.12-2015. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Блочные шифры.
8. ГОСТ Р 34.13-2015. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.
9. Р 50.1.113-2016 «Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования», 2016.
10. Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования», 2018.
11. Р 1323565.1.023-2018 «Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509», 2018.
12. Р 1323565.1.026-2019 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование».
13. Требования к средствам электронной подписи. Приложение к приказу ФСБ России от 27.12.2011 № 796.
14. Средство криптографической защиты информации «Крипто-КОМ 3.5». Правила пользования. ШКНР.00064-01 90 02. АО «СИГНАЛ-КОМ», 2022.
15. Средство криптографической защиты информации «Крипто-КОМ 3.5». Программное обеспечение контроля целостности. Руководство оператора. ШКНР.00064-01 34 01. АО «СИГНАЛ-КОМ», 2022.
16. Средство криптографической защиты информации «Крипто-КОМ 3.5». Утилита удаления файлов. Руководство оператора. ШКНР.00064-01 34 02. АО «СИГНАЛ-КОМ», 2022.
17. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.
18. RFC 5280. D.Cooper, S.Santesson, S.Farrell, S.Boeyen, R.Housley, W. Polk, «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», May 2008.
19. RFC 4357. Additional cryptographic algorithms for use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 algorithms. V.Popov, I.Kurepkin, S.Leontiev, January 2006.
20. ITU-T Recommendation X.680. Information Technology - Abstract Syntax Notation One (ASN.1).
21. Adi Shamir, How to share a secret. Communications of the ACM, 1979.