

ЗАО «Сигнал-КОМ»

УТВЕРЖДЕН  
ШКНР.00046-01 31 02-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ  
«Крипто-КОМ 3.4»

ПОДСИСТЕМА УПРАВЛЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИЕЙ  
для вариантов исполнения 42, 43  
Общее описание

ШКНР.00046-01 31 02

Листов 17

## **АННОТАЦИЯ**

В данном документе рассматриваются вопросы управления ключевой системой, используемой в СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43), с учетом мер, обеспечивающих безопасность использования ключей электронной подписи и ключевого обмена.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «Крипто-КОМ 3.4», должны разрабатываться с учетом требований настоящего документа.

## СОДЕРЖАНИЕ

Аннотация .....	2
Содержание .....	3
1. Общие сведения .....	4
2. Основные технические данные и характеристики .....	5
2.1. Криптографические алгоритмы .....	5
2.1.1. Реализация ГОСТ 28147-89 .....	5
2.1.2. Реализация ГОСТ Р 34.11-94 .....	5
2.1.3. Реализация ГОСТ Р 34.11-2012 .....	5
2.1.4. Реализация ГОСТ Р 34.10-2001 .....	6
2.1.5. Реализация ГОСТ Р 34.10-2012 .....	6
2.2. Ключевые носители .....	6
2.3. Ключевые носители с неэкспортируемыми ключами .....	7
3. Общее описание ключевой системы СКЗИ «Крипто-КОМ 3.4» .....	8
3.1. Ключевая информация .....	8
3.1.1. Симметричные ключи шифрования .....	8
3.1.2. Ключи электронной подписи и ключевого обмена .....	8
3.1.2.1. Ключи ключевого обмена .....	9
3.1.2.2. Ключи электронной подписи .....	9
3.1.3. Сертификаты открытых ключей и списки отозванных сертификатов .....	9
3.2. Ключевая система .....	10
3.2.1. Структура ключевого хранилища .....	10
3.2.2. Формирование ключевой информации .....	11
3.3. Требования к ключевым носителям .....	12
3.4. Длина ключей .....	13
3.4.1. Сроки действия ключей .....	13
3.4.2. Уничтожение ключевых носителей .....	13
4. Рекомендации по управлению ключевой системой .....	14
4.1. Удостоверяющий центр .....	14
4.2. Порядок разбора конфликтных ситуаций, связанных с применением ЭП .....	14
4.2.1. Порядок разбора конфликтной ситуации .....	15
4.2.2. Случаи невозможности проверки значения ЭП .....	15
Литература .....	17

## **1. ОБЩИЕ СВЕДЕНИЯ**

СКЗИ «Крипто-КОМ 3.4» в вариантах исполнения 42, 43 предназначено для криптографической защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в информационных системах общего пользования.

Ключевая система СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) ориентирована на совместное использование одноключевых и двухключевых криптосистем.

## **2. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ И ХАРАКТЕРИСТИКИ**

СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) 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 [13]. Допускается использование СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) для криптографической защиты персональных данных.

### **2.1. Криптографические алгоритмы**

СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) включает реализацию следующих алгоритмов:

- алгоритм создания ЭП - реализован 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].

Ключевая система СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) ориентирована на совместное использование одноключевых и двухключевых криптосистем.

#### **2.1.1. Реализация ГОСТ 28147-89**

В СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) используются четыре режима системы криптографического преобразования в соответствии с ГОСТ 28147-89 [2]:

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

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 34.11-94**

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.

#### **2.1.3. 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.

#### 2.1.4. Реализация ГОСТ Р 34.10-2001

ГОСТ Р 34.10-2001 [3] устанавливает процедуры формирования 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.

СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) реализует только процедуру проверки электронной подписи ГОСТ Р 34.10-2001.

#### 2.1.5. Реализация ГОСТ Р 34.10-2012

ГОСТ Р 34.10-2012 [4] устанавливает процедуры формирования 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 3.4», будем называть ключевой информацией<sup>1</sup>, а магнитные носители и другие внешние устройства, на которые записываются ключи при формировании - *ключевыми носителями*.

Для хранения ключевой информации в СКЗИ «Крипто-КОМ 3.4» могут быть использованы следующие типы ключевых носителей (см. Таблица 1):

Таблица 1

Тип ключевого носителя	Уровень защиты
Накопители на гибком магнитном диске (НГМД)	КС1, КС2
Разделы накопителей на жестком магнитном диске (НЖМД)	КС1, КС2
Сменные носители с интерфейсом USB	КС1, КС2
Электронные ключи с интерфейсом USB (eToken, Rutoken и др.)	КС1, КС2
Криптографические устройства, перечисленные в Таблица 2	КС1, КС2
Карты флэш-памяти	КС1, КС2
Реестр Windows	КС1, КС2

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

<sup>1</sup> Формирование ключевой информации должно выполняться с помощью специализированного программного обеспечения, разработанного с использованием СКЗИ, сертифицированного ФСБ России.

### 2.3. Ключевые носители с неэкспортируемыми ключами

СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) может обращаться через интерфейс PKCS#11 к криптографическим устройствам, реализующим функции генерации ключей, создания ЭП, проверки ЭП, хэширования, шифрования, ключевого обмена, генерации случайных последовательностей и др. Данные устройства могут также использоваться для хранения закрытых ключей в неэкспортируемом виде, исключающем возможность их считывания во внешнюю память или копирование на другой носитель.

СКЗИ «Крипто-КОМ 3.3» (варианты исполнения 42, 43) может использовать механизмы (генерация ключей, создание ЭП, проверка ЭП, хэширование, шифрование, ключевой обмен, генерация случайных последовательностей и др.), реализованные в криптографических устройствах, совместно с программной реализацией криптографических алгоритмов СКЗИ «Крипто-КОМ 3.3» (хэширование, шифрование и др.).

Перечень криптографических устройств, поддерживаемых СКЗИ «Крипто-КОМ 3.3» (варианты исполнения 42, 43), приведён в Таблица 2:

Таблица 2

Тип криптографического устройства	Предприятие-изготовитель
РУТОКЕН ЭЦП	ЗАО «Актив-софт», ООО «АНКАД»
eToken ГОСТ/JaCarta ГОСТ	ЗАО «Аладдин Р.Д.»
ESMART Token ГОСТ	ОАО «НИИМЭ и Завод Микрон»

Примечание. СКЗИ, реализованные с использованием устройств, перечисленных в Таблица 2, должны быть сертифицированы по требованиям ФСБ России к СКЗИ по классу КС1, КС2 или КС3.

### **3. ОБЩЕЕ ОПИСАНИЕ КЛЮЧЕВОЙ СИСТЕМЫ СКЗИ «КРИПТО-КОМ 3.4»**

Ключевая система СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) ориентирована на совместное использование одноключевых и двухключевых криптосистем.

В системах защиты информации, построенных на базе СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43), открытые ключи (ключи проверки ЭП и открытые ключи ключевого обмена) пользователей используются, хранятся и передаются по каналам связи в виде цифровых сертификатов (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 открытыми ключами, обеспечивающей контроль за выполнением всех процедур, связанных с формированием, регистрацией, хранением и обновлением ключевых носителей участников защищенной системы.

Управление открытыми ключами СКЗИ «Крипто-КОМ 3.4» 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 формирующим сертификаты и списки отозванных сертификатов (СОС) в соответствии с Рекомендациями ITU-T X.509 [9] (далее - X.509) и IETF RFC 3280 [10], RFC 4491 [12] (далее - PKIX), а также рекомендациями Технического комитета 026 Росстандарта.

В зависимости от требований политики безопасности эксплуатирующей организации, СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) допускает возможность формирования криптографических ключей пользователей как децентрализованно - самостоятельно самими пользователями на своих рабочих местах, так и централизованно – администратором безопасности.

#### **3.1. Ключевая информация**

##### **3.1.1. Симметричные ключи шифрования**

В СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) для симметричных криптопреобразований используется одноключевой алгоритм шифрования с длиной ключа 256 бит, выполненный в соответствии с требованиями ГОСТ 28147-89 [2] и реализующий следующие 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 информацией СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) использует динамическое формирование симметричных ключей шифрования, удовлетворяющих требованиям ГОСТ 28147-89.

При динамической генерации симметричные ключи формируются по мере необходимости приложениями, построенными на базе СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43), с использованием методов открытого распределения ключей.

##### **3.1.2. Ключи электронной подписи и ключевого обмена**

СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) поддерживает криптосистемы с открытым распределением ключей, предполагающие наличие у каждого пользователя пары ключей - закрытого и открытого.

В приложениях на базе СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43), 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 3.4» (варианты исполнения 42, 43) для зашифрования и расшифрования информации используется общий секретный ключ связи (в соответствии с ГОСТ 28147-89). Формирование 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 3.4» (варианты исполнения 42, 43) для формирования электронной 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 формировании электронной подписи используется ключ ЭП пользователя, а при проверке подписи – его ключ проверки ЭП. В процессе формирования подписи исходное сообщение произвольного объема преобразуется в хэш-значение длиной 256 или 512 бит.

#### **3.1.3. Сертификаты открытых ключей и списки отозванных сертификатов**

В асимметричных криптосистемах, построенных на базе СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43), открытый ключ (ключ проверки ЭП и открытый ключ ключевого обмена) можно использовать только при условии достоверного подтверждения его подлинности (отсутствие искажений и принадлежность определенному лицу), что может быть обеспечено:

- заверением открытого ключа третьей доверенной стороной (использование открытого ключа в составе цифрового сертификата, заверенного Удостоверяющим центром, или нотариальное заверение копии открытого ключа на бумажном носителе, собственноручно подписанном владельцем ключа);
- обменом открытыми ключами взаимодействующих сторон при их личной встрече;
- доверенным распространением и хранением открытых ключей в виде справочников.

Цифровым сертификатом открытого ключа называется структурированный двоичный набор данных в формате, определенном Рекомендациями ITU-T X.509 [9], включающий следующую информацию:

- уникальный серийный номер сертификата;
- идентификатор алгоритма, используемого для подписи;
- уникальное имя издателя сертификата;
- даты начала и окончания срока действия сертификата;
- имя пользователя или объекта системы, однозначно идентифицирующего его в рамках данной системы;
- информацию об открытом ключе пользователя или объекте системы: идентификатор алгоритма и собственно открытый ключ;
- 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 (сертификат ключа проверки ЭП) 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 3.4» (варианты исполнения 42, 43) сертификатом может служить цифровой сертификат открытого ключа в формате X.509, а также учетная карточка, представляющая собой бумажный бланк, на котором распечатаны открытый ключ и реквизиты пользователя, заверенные печатью и подписью уполномоченного лица УЦ (администратора или администратора безопасности).

Открытые ключи пользователей передаются на регистрацию и последующую сертификацию в УЦ в составе запроса на сертификат. Запросы на сертификаты могут формироваться приложениями, построенными на базе СКЗИ «Крипто-КОМ 3.4».

При работе с открытыми ключами пользователю необходимо иметь справочник открытых ключей 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 открытых ключей.

Регламент работы со справочниками открытых ключей 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 открытых ключей 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 открытых ключей старые справочники с открытыми ключами подписи необходимо сохранять в архиве для последующих процедур разбора конфликтных ситуаций (см. п. 4.2);
- чтобы исключить подделку справочника сертификатов, при каждом использовании сертификата открытого ключа должна выполняться проверка подписи УЦ под сертификатом.

УЦ может отозвать (заблокировать) выданный им сертификат (например, в случае компрометации соответствующего закрытого ключа). Для доведения до пользователей информации об отозванных сертификатах УЦ выпускает списки отозванных сертификатов (СОС), заверенные электронной подписью УЦ и включающие в себя перечень серийных номеров сертификатов, отозванных на определенный момент времени.

Чтобы исключить возможность использования скомпрометированного или отозванного сертификата, наряду с проверкой подписи УЦ под сертификатом должен выполняться поиск ссылки на данный сертификат в списке отозванных сертификатов и проверка подписи УЦ под списком.

## **3.2. Ключевая система**

### **3.2.1. Структура ключевого хранилища**

В «Крипто-КОМ 3.4» (варианты исполнения 42, 43) 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 - КЕК); зашифрован на главном ключе;
- вектор состояния (инициализирующая последовательность) для программного датчика случайных чисел (может отсутствовать, см. п. 3.2.2); зашифрован на КЕК;
- произвольное количество ключей электронной подписи и ключевого обмена, зашифрованных на КЕК.

В хранилище реализован механизм контроля целостности объектов с использованием имитовставки, вычисляемой по ГОСТ 28147-89.

СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) 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 3.4» (варианты исполнения 42, 43) могут использовать дополнительные методы защиты ключевой информации (например, парольную защиту либо организационно-техническое разделение ключа на несколько частей).

### **3.2.2. Формирование ключевой информации**

В СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) ключи ЭП и закрытые ключи ключевого обмена формируются с помощью аппаратного или программного датчика случайных чисел (ДСЧ).

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

- ПАК защиты от НСД «Соболь» (версии кода расширения BIOS 1.0.99, 1.0.180);
- СЗИ НСД «Аккорд-АМД3» (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 генерации случайных чисел автоматически определяет наличие одного из перечисленных устройств и устанавливает соответствующий метод генерации случайных чисел.

Программный датчик случайных чисел (ПДСЧ) строится на основе гаммирования по алгоритму ГОСТ 28147-89 и может быть инициализирован:

- от физического датчика случайных чисел перечисленных выше программно-аппаратных средств защиты информации;
- от программно-клавиатурной компоненты (биологический ДСЧ);
- от вектора состояния (инициализирующей последовательности) ПДСЧ, сохраненного в контексте ключевого контейнера.

При инициализации биологического ДСЧ пользователю предлагается ввести символы с клавиатуры (дополнительно могут использоваться события от манипулятора «мышь»). После ввода пользователем символа (или по событию от «мыши») производится считывание значения счетчика тактов процессора. В процессе инициализации производится оперативный статистический контроль качества значений счетчика тактов процессора и автоматически определяется необходимое количество попыток. Дополнительно могут считываться значения других счетчиков: счетчиков системного времени и циклических счетчиков, запускаемых в отдельных потоках. Результаты попыток независимо друг от друга обрабатываются с помощью функции хэширования по ГОСТ Р 34.11-94, а в конце работы алгоритма складываются по модулю 2. Результатом работы алгоритма является 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 Таблица 2.

Выбор способа формирования ключей при работе с СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) определяется регламентом работы сети конфиденциальной связи и требованиями к уровню защищенности СКЗИ (КС1 или КС2), установленного на рабочем месте владельца ключей.

---

<sup>1</sup> Перечень источников аппаратно-генерируемых случайных чисел может изменяться и расширяться.

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

Подсистема управления ключевой информацией СКЗИ «Крипто-КОМ 3.4» допускает несколько способов формирования асимметричных (закрытый и открытый) ключей пользователей, отличающихся

режимом формирования:

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

типом ДСЧ, используемого при генерации ключей:

- физический ДСЧ одного из ПАК защиты от НСД, сертифицированных ФСБ России;
- программный ДСЧ из состава СКЗИ «Крипто-КОМ 3.4»;
- ДСЧ криптографических устройств, перечисленных в Таблица 2.

В подсистеме управления ключевой информацией СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43), сформированные открытые ключи пользователей передаются на сертификацию в УЦ.

### **3.3. Требования к ключевым носителям**

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

Закрытые ключи (ключи ЭП и закрытые ключи ключевого обмена) пользователя относятся к конфиденциальной информации. Пользователь должен обеспечить надежное хранение в тайне своего закрытого ключа.

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 закрытых ключей 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 3.4» (варианты исполнения 42, 43) 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 ЭП по ГОСТ Р 34.10-2001 – 256 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.

#### **3.4.1. Сроки действия ключей**

В СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43) допускаются следующие сроки действия ключей:

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

Возможность увеличения срока действия закрытых ключей может быть рассмотрена при условии обеспечения дополнительных организационно-технических мер защиты, исходя из конкретных условий эксплуатации, в процессе проведения какой-либо из следующих работ:

- оценка влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к ним требований;
- тематические исследования СКЗИ, построенного на базе СКЗИ «Крипто-КОМ 3.4» (варианты исполнения 42, 43).

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

#### **3.4.2. Уничтожение ключевых носителей**

Закрытые ключи (ключи ЭП и закрытые ключи ключевого обмена), 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 3.4» (варианты исполнения 42, 43), предназначенная для удаления файлов с ключевых носителей с предварительным их физическим затиранием. Порядок использования утилиты приводится в документе [8].

Дискеты, 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, открытые ключи проверки ЭП должны сохраняться в архиве открытых ключей 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 3.4» (варианты исполнения 42, 43), УЦ представляет собой организационно-административную структуру, отвечающую за проведение политики информационной безопасности.

Использование УЦ обеспечивает выполнение всех необходимых процедур администрирования, связанных с формированием, регистрацией, хранением, обновлением и распространением открытых ключей (ключей проверки ЭП, открытых ключей ключевого обмена) 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]:

- генерация ключей ЭП и ключей проверки ЭП УЦ (уполномоченного лица УЦ);
- формирование корневых (самоподписанных) сертификатов ключей проверки ЭП УЦ;
- формирование 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 издание сертификатов открытых ключей пользователей;
- верификация запросов и контроль уникальности открытых ключей в регистрируемых запросах;
- формирование сертификатов открытых ключей пользователей;
- выдача сертификатов открытых ключей пользователей в электронной форме и в форме документов на бумажных носителях;
- сохранение запросов на сертификаты в течение установленного срока хранения;
- доставка сертификатов открытых ключей пользователям;
- приостановление и возобновление действия сертификатов, а также их аннулирование;
- изготовление списков отозванных сертификатов пользователей (СОС);
- ведение реестра выпущенных сертификатов и списков отозванных сертификатов;
- 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 3.4» (варианты исполнения 42, 43), должны быть сертифицированы по «Требованиям к средствам удостоверяющего центра» [15].

### **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 формирования 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 закрытым ключом электронной подписи.

При проверке значения ЭП используется ключ проверки ЭП, парный ключу ЭП, с помощью которого выполнялась процедура формирования 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 или нескольких сертификатов, необходимых для проверки ЭП;
- проверка ЭП электронного документа с использованием каждого сертификата;
- проверка ЭП каждого сертификата, путем построения цепочки сертификатов до сертификата главного (корневого) УЦ;
- проверка действительности сертификатов на текущий момент времени;
- проверка действительности сертификатов на момент формирования ЭП;
- проверка отсутствия сертификатов в СОС.

Если сертификат, с использованием которого проверяется ЭП, отозван (т.е. включен в СОС), комиссия принимает решение о действительности ЭП документа, используя дату создания документа и дату отзыва сертификата в СОС.

При проверке ЭП документа, верификации цепочки сертификатов, отсутствии сертификата в СОС, составляется «Протокол проверки ЭП», в котором фиксируются сертификаты ключей проверки ЭП, использованные для проверки, и факт подтверждения или неподтверждения подписи. 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, указанных в протоколе проверки, необходимо сравнить со значениями ключей проверки ЭП соответствующих бумажных копий, заверенных администратором УЦ. При совпадении их значений, авторство подписи под документом считается установленным.

#### **4.2.2. Случай 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. СКЗИ «Крипто-КОМ 3.4». Программное обеспечение контроля целостности. Руководство пользователя. ШКНР.00046-01 90 05.
8. СКЗИ «Крипто-КОМ 3.4». Утилита для удаления файлов. Руководство пользователя. ШКНР.00046-01 90 06.
9. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.
10. RFC 3280. Housley, W. Polk, W. Ford, D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002
11. RFC 3039. S.Santesson, W. Polk, P.Barzin, M.Nystrom, Internet X.509 Public Key Infrastructure Qualified Certificates Profile, January 2001.
12. RFC 4491. S. Leontiev, D. Shefanovski, Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2006.
13. СКЗИ «Крипто-КОМ 3.4». Правила пользования. ШКНР.00046-01 90 03.
14. Adi Shamir, How to share a secret. Communications of the ACM, 1979.
15. Требования к средствам удостоверяющего центра». Приложение к приказу ФСБ России от 27.12.2011 № 796.