127 018, Москва, Сущевский Вал, д.18
Телефон: (495) 9954820
Факс: (495) 995 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

КРИПТОПРО

Средство Криптографической Защиты Информации

КриптоПро CSP

Версия 4.0 R4 КС1

1-Base

Руководство администратора безопасности

Общая часть

ЖТЯИ.00087-03 91 01
Листов 81

2018 г.

‹ **ООО** © ò ø ð ÷ ú ë ÷ ø ö ª **-2018.** ê ! ! #

Авторские права на средства криптографической защиты информации типа «КриптоПро CSP» и эксплуатационную документацию зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент).

Настоящий документ входит в комплект поставки программного обеспечения СКЗИ «КриптоПро CSP» версии 4.0 R4; на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО «КРИПТО-ПРО» документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

Содержание

1. Назначение СКЗИ 20
2. Требования к эксплуатации СКЗИ 21
3. Программно-аппаратные среды функционирования СКЗИ 22
4. Реализуемые криптографические алгоритмы 24
5. Структура и состав СКЗИ 25
5.1. Структура СКЗИ 25
5.2. Состав СКЗИ 26
5.3. Состав программного обеспечения СКЗИ 26
5.4. Состав подсистемы программной СФК 26
5.5. Получение прав на использование СКЗИ «КриптоПро CSP» 27
Ключевая система и ключевые носители 28
5.6. Общие положения 28
5.6.1. Шифрование данных 28
5.6.2. Формирование и проверка ЭП 28
5.7. Ключевой контейнер 28
5.8. Формат ключевого контейнера 29
5.9. Формирование ключей 29
5.10. Ключевые носители 30
5.11. Размеры ключей 31
5.12. Хранение ключевых носителей 31
5.13. Сроки действия пользовательских ключей 32
5.14. Уничтожение ключей на ключевых носителях 33
5.15. Интерфейс управления ключами СКЗИ 33
6. Протокол сетевой аутентификации «КриптоПро TLS» 34
6.1. Основные понятия протокола TLS 35
6.2. Модуль сетевой аутентификации «КриптоПро TLS» 38
6.3. Проверка использования российских алгоритмов в браузере Internet Explorer/Edge 39
7. Управление ключами СКЗИ 42
7.1. Удостоверяющий центр 42
7.2. Формирование ключей Центра Сертификации 43
7.3. Хранение и использование закрытого ключа ЦС 43
7.4. Формирование ключей Центра Регистрации 44
7.4.1. Регистрация Центра Регистрации 44
7.4.2. Изготовление ключей Центра Регистрации 44
7.5. Формирование ключей пользователя 44
7.5.1. Регистрация пользователя 44
7.5.2. Формирование личных ключей пользователя 45
7.5.3. Получение личного сертификата пользователем 46
7.6. Повторная регистрация пользователя 46
7.7. Плановая смена ключей 46
7.7.1. Смена ключей Центра Сертификации 46
7.7.2. Смена ключей Центра Регистрации 47
7.7.3. Смена ключей пользователя 47
7.8. Компрометация ключей 47
7.8.1. Компрометация ключей Центра Сертификации 47
7.8.2. Компрометация ключей Центра Регистрации 47
7.8.3. Компрометация ключей пользователя 48
7.8.4. Действия УЦ при компрометации ключей пользователя 48

7.9. Исключение пользователя из сети ... 48
7.10. Периодичность издания СОС ... 49
7.11. Ведение журналов ... 49
8. Разбор конфликтных ситуаций, связанных с применением ЭП ... 50
8.1. Порядок разбора конфликтной ситуации ... 50
8.2. Случаи невозможности проверки значения ЭП ... 51
9. Нештатные ситуации при эксплуатации СКЗИ ... 52
10. Применение «КриптоПро CSP» v. 4.0 R4 ... 54
11. Использование СКЗИ в стандартном программном обеспечении ... 55
12. Использование СКЗИ с программными продуктами разработки ООО «КРИПТО-ПРО» ... 58
13. Встраивание СКЗИ ... 59
14. Требования по защите от НСД ... 60
14.1. Общие требования по организации работ по защите от НСД ... 60
14.2. Требования по размещению технических средств с установленным СКЗИ ... 60
14.3. Требования по установке СКЗИ, общесистемного и специального ПО на ПЭВМ ... 60
14.4. Меры по обеспечению защиты от НСД ... 61
14.5. Требования по подключению СКЗИ для работы по общедоступным каналам передачи данных ... 64
14.6. Требования по использованию в СКЗИ программно-аппаратных средств защиты от НСД 64
14.6.1. Электронный замок «Соболь» ... 65
15. Требования по криптографической защите ... 66
16. Требования по встраиванию и использованию ПО СКЗИ ... 67
Литература ... 69
Приложение А. Акт готовности к работе. ... 70
Приложение Б. Журнал регистрации администраторов безопасности и пользователей ... 71
Приложение В. Журнал пользователя сети ... 72
Приложение Г. «Удостоверяющий центр «КриптоПро УЦ» ... 73

Аннотация

Настоящее Руководство содержит общее описание средства криптографической защиты информации «КриптоПро CSP» v. 4.0 R4 (ЖТЯИ.00087-03) исполнения 1-Base и рекомендации по использованию СКЗИ в различных автоматизированных системах.

В зависимости от комплектации и используемой программно-аппаратной среды функционирования СКЗИ следует руководствоваться также документами [9] - [22].

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих «КриптоПро CSP» v. 4.0 R4, должны разрабатываться с учетом требований настоящего Руководства.

Список сокращений

CRL (СОС)	Certificate Revocation List - Список отозванных сертификатов
IETF	Internet Engineering Task Force
АРМ	Автоматизированное рабочее место
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Hard Disk Drive - Жесткий магнитный диск
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
Регистрация	Присвоение определенных атрибутов (адреса, номера ключа, прав использования и т.п.) абоненту
Регламент	Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах.
Сертификат	Электронный документ, подтверждающий принадлежность открытого ключа или ключа проверки электронной подписи и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата открытого ключа или ключа проверки электронной подписи абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СС	Справочник сертификатов открытых ключей и ключей проверки электронной подписи. Сетевой справочник.
СФК	Среда функционирования комплекса
ЦС	Центр Сертификации УЦ
УЦ	Удостоверяющий Центр
ЦР	Центр Регистрации УЦ
ЭД	Электронный документ
ЭП	Электронная подпись

Основные термины и понятия

Автоматизированная информационная система

Комплекс программных и технических средств, предназначенных для сбора, хранения, поиска и выдачи информации по запросам.

Автоматизированная система

Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Авторство информации

Однозначное соответствие между содержанием и/или формой информации и субъектом (объектом), сформировавшим эту информацию. Для пользователя авторство полученной им из системы или канала связи информации означает однозначное установление источника, сформировавшего эту информацию (ее автора).

Актуальность информации

Свойство информации сохранять свои свойства (ценность) для субъекта (пользователя) в течение определенного периода времени.

Администратор безопасности

Субъект доступа, основной обязанностью которого является обеспечение безопасности конфиденциальной связи на том участке сети, которую он курирует. Система административного управления безопасностью включает в себя комплекс организационно-технических мер, направленных на обеспечение конфиденциальности связи.

Основные направления деятельности администратора безопасности:

– контроль целостности программного обеспечения;

– управление ключевой системой: хранение, ввод в действие и смена ключей пользователей, генерация закрытых и открытых ключей подписи пользователей, ключей электронной подписи, ключей проверки электронной подписи;

– управление доступом пользователей системы к программному обеспечению и данным, включая установку и периодическую смену паролей, управление средствами защиты коммуникаций, передаваемых, хранимых и обрабатываемых данных.

Администратор защиты

Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Аутентификация информации

Установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации, установление законным получателем (возможно арбитром) факта, что полученная информация наиболее вероятно была передана законным отправителем (источником) и что она при этом не заменена и не искажена. Любые преднамеренные и случайные попытки искажений информации обнаруживаются с соответствующей вероятностью.

Безопасность

Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба.

Безопасность информации (информационная безопасность)

Состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п..

Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

Блокирование информации

Прекращение или затруднение доступа законных пользователей к информации.

Верификация

Установление соответствия принятой и переданной информации с помощью логических методов.

процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие.

Владелец информации

Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

Субъект информационных отношений, обладающий правом владения, распоряжения и пользованием информационным ресурсом по договору с собственником информации.

Владелец информации, информационной системы

Субъект, в непосредственном ведении которого в соответствии с законом находятся информация, информационная структура.

Государственная тайна

Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Гриф конфиденциальности

Специальная отметка на носителе информации либо в сопроводительных документах на него, свидетельствующая о том, что носитель содержит конфиденциальную информацию.

Гриф секретности

Реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и/или в сопроводительной документации на него.

Документ

Документированная информация, снабженная определенными реквизитами.

Материальный объект с информацией, закрепленной созданным человеком способом для ее передачи во времени и пространстве.

Документированная информация (документ)

Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

÷ . Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

Документ в электронной форме (Электронный документ)

Электронный образ документа (платежного или иного) - файл, достоверность которого обеспечивается комплексом мероприятий по защите информации. При этом файл может содержать несколько документов (пакет документов).

ЭД представляет собой документированную совокупность данных, зафиксированных на материальном носителе (магнитном или бумажном) с реквизитами, позволяющими идентифицировать эту информацию и авторов документа. Идентификация ЭД обеспечивается средствами защита на основе алгоритмов шифрования, электронной подписи и защиты от несанкционированного доступа.

ЭД создается участником системы на основе бумажного документа либо на основании другого электронного документа и полностью повторяет его по содержанию. ЭД обрабатываются и хранятся в ЭВМ и могут передаваться по электронным каналам связи.

Доступ к информации

Получение субъектом возможности ознакомления с информацией, в том числе с помощью технических средств.

Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Доступность информации

Свойство информации, технических средств и технологии обработки, характеризующееся способностью обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

Заверение (нотаризация)

Регистрация данных у доверенного третьего лица для повышения уверенности в правильности таких характеристик, как содержание, источник данных, время доставки.

Защита информации

Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкциониро-ванного копирования, блокирования информации.

Защита информации от НСД

Составная часть общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа. В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД, условно состоящей из следующих четырех подсистем: управления доступом; регистрации и учета; криптографической; обеспечения целостности.

Защищенное средство вычислительной техники (защищенная автоматизированная система)

Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.

IA32, IA64, x64, SPARC, Power PC

Аппаратные платформы, используемые производителями ПЭВМ

Идентификация

Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Имитозащита

Защита системы шифрованной связи от навязывания ложных данных.

Имитовставка

Отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты.

Квалифицированный сертификат ключа проверки электронной подписи

Сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Ключ (криптографический ключ)

Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований [2].

Ключ проверки электронной подписи

Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключ электронной подписи

Уникальная последовательность символов, предназначенная для создания электронной подписи.

Компрометация ключа

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

1. Потеря ключевых носителей.
2. Потеря ключевых носителей с их последующим обнаружением.
3. Увольнение сотрудников, имевших доступ к ключевой информации.
4. Нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа.
5. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
6. Нарушение печати на сейфе с ключевыми носителями.
7. Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)

Различаются два вида компрометации закрытого ключа: ' ' и ' ' . Первые четыре события трактуются как явная компрометация ключей. Следующие три требуют специального рассмотрения в каждом конкретном случае.

Конфиденциальность информации

Субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

Конфиденциальная информация

Документированная информация, доступ к которой ограничивается в соответствии с Законодательством РФ. Другая информация, требующая защиты.

Контроль доступа (управление доступом)

Процесс ограничения доступа к ресурсам системы только разрешенным субъектам или объектам.

Криптографическая защита

Защита данных при помощи криптографических преобразований данных.

Криптопровайдер

Реализует функции шифрования, вычисления имитовставки, хэширования, формирования и проверки подписи, генерации пользовательских ключей. Обеспечивает работу с сессионными ключами шифрования (генерация, экспорт/импорт в защищенном виде), закрытыми и открытыми ключами ЭП и обмена, ввод ключей с ключевых носителей, защищённое хранение и уничтожение ключей в оперативной памяти. Реализуется как библиотека, динамически загружаемая в единое адресное пространство процесса, инициируемого прикладной задачей.

Криптопродрайвер

Реализует функции шифрования и вычисления имитовставки, хэширования и проверки подписи. Обеспечивает работу с сессионными ключами шифрования (генерация, экспорт/импорт в защищенном виде), ключами проверки ЭП, эфемерными закрытыми и

открытыми ключами обмена, защищённое хранение и уничтожение ключей в оперативной памяти. Загружается в адресное пространство ядра ОС.

По своему интерфейсу и функциональным возможностям криптодрайвер обеспечивает возможности криптопровайдера за исключением функций формирования цифровой подписи, работы с носителем ключей, генерации ключей пользователя. Позволяет организовывать шифрование данных и проверку цифровой подписи на уровне ядра операционной системы и ускорить криптографические операции с потоком данных за счет исключения из процесса обработки данных их пересылку с уровня ядра на уровень приложений и обратно.

Криптосервис

Процесс, запускаемый в собственном адресном пространстве. Криптосервис, как и криптопровайдер, выполняет все криптографические функции, включая генерацию ключей пользователя. Криптосервис может использоваться несколькими процессами. Взаимодействие криптосервиса с процессами осуществляется по протоколу RPC в режиме разделения клиентов. Ключевая информация с носителей всех клиентов кэшируется в несвопируемую часть адресного пространства криптосервиса.

Криптографическое преобразование

Преобразование информации с использованием криптографических алгоритмов.

Лицензирование в области защиты информации

Деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации.

Мероприятия по защите информации

Совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

Мероприятия по контролю эффективности защиты информации

Совокупность действий по разработке и/или практическому применению способов и средств контроля эффективности защиты информации.

Метка конфиденциальности

Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте.

Нарушитель безопасности информации

Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами.

Нарушитель правил разграничения доступа

Субъект доступа, осуществляющий несанкционированный доступ к информации.

Некорректный электронный документ

Электронный документ, не прошедший процедуры расшифрования данных, проверки электронной подписи информация, контроля формата документов, а также документ, имеющий искажения в тексте сообщения (наличие символов, букв или цифр в расшифрованном (открытом) тексте документа, не позволяющих понять его смысл).

Непреднамеренное воздействие на информацию

Ошибка пользователя, сбой технических и программных средств информационных систем, а также природное явление или иное нецеленаправленное на изменение информации воздействие, связанное с функционированием технических средств, систем или с деятельностью людей, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Несанкционированное воздействие на информацию

Воздействие на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящее к искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Несанкционированный доступ к информации (НСД)

1. Получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

2. Доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или автоматизированной системы (АС).

Носитель информации

Физическое лицо или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Объект доступа

Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Объект защиты

1. Информация или носитель информации, или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

2. Информация, технические средства и технология ее обработки, в отношении которых необходимо обеспечить безопасность информации.

Обработка информации

Передача, прием, хранение, преобразование и отображение информации.

Организация защиты информации

Содержание и порядок действий по обеспечению защиты информации.

Открытый ключ

Криптографический ключ, который связан с закрытым с помощью особого математического соотношения. Открытый ключ известен всем другим пользователям системы и предназначен для проверки электронной подписи и расшифрования, позволяет определить автора подписи и достоверность электронного документа, но не позволяет вычислить закрытый ключ. Открытый ключ считается принадлежащим пользователю, если он был зарегистрирован (сертифицирован) установленным порядком.

Пароль

1. Идентификатор субъекта доступа, который является его (субъекта) секретом.

2. Секретная информация аутентификации, обычно представляющая собой строку знаков, которой должен обладать пользователь для доступа к защищенным данным.

Плановая смена ключей

Смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

Побочные электромагнитные излучения и наводки

1. Электромагнитные излучения технических средств обработки информации, не предназначенные для передачи, приема или преднамеренного искажения информации, а также наводки от технических средств в окружающих предметах.

2. Нежелательные излучения и наводки, проявляющиеся в виде побочных, внеполосных, шумовых и наводимых сигналов, потенциально образующих неконтролируемые каналы утечки конфиденциальной информации.

Побочное электромагнитное излучение

Нежелательное информационное электромагнитное излучение, возникающее в результате нелинейных процессов в электрических цепях при обработке информации техническими средствами и приводящие к утечке информации.

Пользователи

Граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения обладают равными правами на доступ к государственным ресурсам и не обязаны обосновывать перед владельцем этих ресурсов необходимость получения запрашиваемой ими информации. Исключение составляет информация с ограниченным доступом.

Пользователь (потребитель) информации

1. Субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

2. Субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

Полномочный представитель организации

Представитель организации из числа первых должностных лиц в соответствии с уставным документом или, имеющий соответствующую доверенность.

Правило доступа к защищаемой информации

Совокупность правил, регламентирующих порядок и условия доступа к защищаемой информации и ее носителям.

Правила разграничения доступа (ПРД)

Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Право доступа к защищаемой информации; право

Совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации.

Проверка электронной подписи документа

Проверка соотношения, связывающего хэш-функцию документа, подпись под этим документом и ключ проверки электронной подписи подписавшего пользователя. Если рассматриваемое соотношение оказывается выполненным, то подпись признается правильной, а сам документ - подлинным, в противном случае документ считается измененным, а подпись под ним - недействительной.

Разглашение

Несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к этой информации.

Расшифрование данных

Процесс преобразования зашифрованных данных в открытые данные при помощи шифра.

Регламентация

Способ защиты информации в процессе функционирования системы мероприятий, создающих такие условия переработки защищаемых данных, при которых возможности несанкционированного доступа сводятся к минимуму. Считается, что для эффективной защиты необходимо строго регламентировать здания, помещения, размещение аппаратуры, организацию и обеспечение работы всего персонала, связанного с обработкой конфиденциальной информации.

Санкционированный доступ к информации

Доступ к информации, не нарушающий правила разграничения доступа.

Сертификат защиты

Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и/или распространение их как защищенных].

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификат открытого ключа

Сертификат ключа проверки электронной подписи или шифрования представляет собой структурированную двоичную запись в формате ASN.1, состоящую из:

- имени субъекта или объекта системы, однозначно идентифицирующей его в системе;
- открытого ключа субъекта или объекта системы;
- дополнительных атрибутов, определяемых требованиями использования сертификата в системе;
- ЭП Издателя (Удостоверяющего центра), заверяющую совокупность этих данных.

Формат сертификата определен в рекомендациях ITU-T .509 и рекомендациях IETF RFC 2459. В настоящее время основным принятым форматом является формат версии 3, позволяющий определить дополнения (**extensions**), с помощью которых реализуется определенная политика безопасности в системе.

Сертификат соответствия

Документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям.

Секретный (закрытый) ключ

Криптографический ключ, который хранится пользователем системы в тайне. Он используется для шифрования.

Система защиты информации

Совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Система защиты информации от НСД

Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Служебная и коммерческая тайна

1. Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными Гражданским кодексом РФ и другими законами. Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Собственник информации

1. Субъект информационных отношений, обладающий юридическим правом владения, распоряжения и пользования информационным ресурсом. Юридическое право владения, распоряжения и пользования информационным ресурсом принадлежит лицам, получившим этот информационный ресурс по наследству. Авторам открытий, изобретений, научно-технических разработок, рационализаторских предложений и т.д.

принадлежит право владения, распоряжения и пользования информацией, источником которой они являются.

2. Субъект, в полном объеме реализующий полномочия владения, пользования и распоряжения информацией в соответствии с законодательными актами.

3. Юридическое или физическое лицо, владеющее информацией в соответствии с Законом о собственности.

Способ защиты информации

Порядок и правила применения определенных принципов и средств защиты информации.

Способы несанкционированного доступа

1. Приемы и порядок действий с целью получения (добывания) охраняемых сведений незаконным путем. К ним, в том числе, относятся:

- инициативное сотрудничество (предательство, измена).
- склонение (принуждение, побуждение) к сотрудничеству (подкуп, шантаж);
- подслушивание переговоров;
- незаконное ознакомление;
- хищение;
- подделка (модификация);
- уничтожение (порча, разрушение);
- незаконное подключение к системам и линиям связи и передачи информации;
- перехват акустических и электромагнитных сигналов;
- визуальное наблюдение;
- фотографирование;
- сбор и анализ документов, публикаций и промышленных отходов.

2. К основным способам НСД относятся:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

3. модификация средств защиты, позволяющая осуществить НСД;

4. внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

Средства вычислительной техники

Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Средство защиты информации

Техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Средство защиты от несанкционированного доступа

Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

Средство криптографической защиты информации

Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Субъект доступа

Лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Субъект информационных отношений

Физическое или юридическое лицо, обладающее определенным правом по отношению к информационному ресурсу. В зависимости от уровня полномочий субъект

информационных отношений может быть источником, собственником, владельцем или пользователем информации.

Техническое средство обработки информации

Техническое средство, предназначенное для приема, накопления, хранения, поиска, преобразования, отображения и передачи информации по каналам связи.

Угроза безопасности

Совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Удостоверяющий центр

Центр управления открытыми ключами и ключами проверки электронной подписи в соответствии с рекомендациями X.509 в части использования сертификатов открытых ключей.

Уничтожение информации

Действие, в результате которого информация перестает физически существовать в технических средствах ее обработки.

Управление ключами

Создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учет и применение в соответствии с политикой безопасности.

Утечка информации

1. Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведкой.

2. Неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация доверена.

Функция хэширования

Заключается в сопоставлении произвольного набора данных в виде последовательности двоичных символов и его образа фиксированной небольшой длины, что позволяет использовать эту функцию в процедурах электронной подписи для сокращения времени подписи и проверки подписи. Эффект сокращения времени достигается за счет вычисления подписи только под образом подписываемого набора данных.

Целостность информации

1. Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Цель защиты информации

Заранее намеченный результат защиты информации.

1. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

2. Целями защиты являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение угроз безопасности личности, общества, государства; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах, сохранение государственной тайны конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в

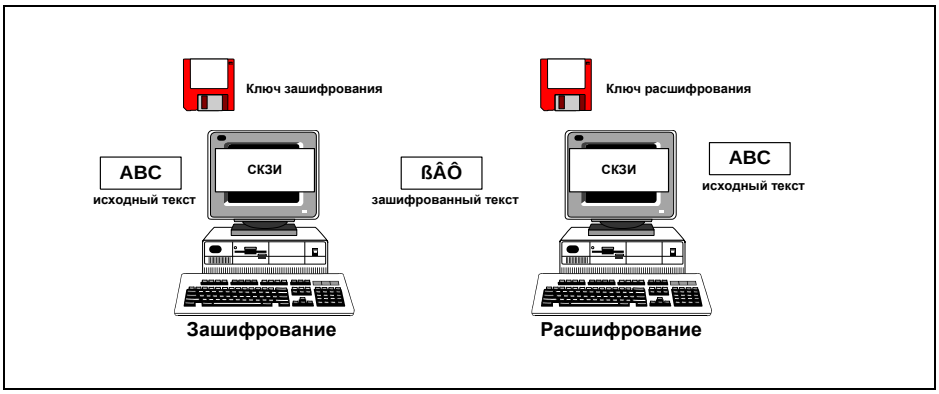
информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Шифр

Совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей.

Шифрование

Процесс зашифрования или расшифрования.



ø **1**

Шифрование информации – взаимнооднозначное математическое (криптографическое) преобразование, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации, представленной в некоторой цифровой кодировке, блок шифрованной информации, также представленной в цифровой кодировке. Термин шифрование объединяет в себе два процесса: зашифрование и расшифрование информации.

Если зашифрование и расшифрование осуществляются с использованием одного и того же ключа, то такой алгоритм криптографического преобразования называется симметричным, в противном случае — асимметричным.

Прочитать зашифрованное сообщение (информацию) может только пользователь, имеющий тот же закрытый ключ шифрования.

Шифрование документов (текстов)

Преобразование формы исходных (открытых) текстов сообщений таким образом, что их смысл становится непонятным для любого лица, не владеющего секретом обратного преобразования.

Шифровальные средства

К шифровальным (криптографическим) средствам (средствам криптографической защиты информации), включая документацию на эти средства, относятся:

а) средства шифрования - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;

б) средства имитозащиты - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации;

в) средства электронной подписи;

г) средства кодирования - средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с

использованием автоматизированных средств, предназначенных для выполнения таких операций;

д) средства изготовления ключевых документов - аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств;

е) ключевые документы - электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах;

ж) аппаратные шифровальные (криптографические) средства - устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин;

з) программные шифровальные (криптографические) средства - программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств;

и) программно-аппаратные шифровальные (криптографические) средства - устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.

Шифрующая файловая система

Файловая система, позволяющая обеспечивать криптографическую защиту файла (шифрование) независимо от других файлов с возможностью его изменения независимо каждым из допущенных к нему пользователей:

Электронная подпись

Данные, добавляемые к блоку данных полученные в результате его криптографического преобразования, зависящего от закрытого ключа и блока данных, которые позволяют приемнику данных удостовериться в целостности блока данных и подлинности источника данных, а также обеспечить защиту от подлога со стороны приемника данных.

Проверка электронной подписи под блоком открытой информации производится с помощью криптографического преобразования и открытого ключа (ключа проверки ЭП), соответствующего закрытому (ключу ЭП), участвовавшего в процессе установки ЭП.

ø **2** ü ÷

Электронная подпись обеспечивает целостность сообщений (документов), передаваемых по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения, с гарантированной идентификацией ее автора (лица, подписавшего документ). Электронная подпись позволяет заменить при безбумажном документообороте традиционные печать и подпись. При построении цифровой подписи вместо обычной связи между печатью или рукописной подписью и листом бумаги выступает сложная математическая зависимость между электронным документом, ключами ЭП и проверки ЭП.

Практическая невозможность подделки электронной подписи опирается на очень большой объем определенных математических вычислений.

Проставление подписи под документом не меняет самого документа, она только дает возможность проверить подлинность и авторство полученной информации.

1. Назначение СКЗИ

СКЗИ предназначено для защиты открытой информации в информационных системах общего пользования (создание/проверка электронной подписи) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах с выполнением следующих функций:

1) защищенное хранение пользовательских ключей в ключевом контейнере с использованием шифрования, имитозащиты и аутентификации доступа;

2) шифрование, вычисление имитовставки, хэширование, создание/проверка электронной подписи данных в областях памяти;

3) формирование сессионных ключей, ключей обмена и ключей создания/проверки ЭП, их импорт/экспорт из/в ключевой контейнер;

4) идентификация, аутентификация, шифрование и имитозащита TLS-соединений;

5) аутентификация в домене Windows с использованием «КриптоПро Winlogon»;

2. Требования к эксплуатации СКЗИ

СКЗИ «КриптоПро CSP» v 4.0 R4 предназначено для защиты открытой информации в информационных системах общего пользования (создание/проверка электронной подписи) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах (шифрование/расшифрование информации, вычисление/проверка имитовставки, вычисление значения хэш-функции, вычисление/проверка электронной подписи).

Средствами СКЗИ «КриптоПро CSP» v 4.0 R4 ' обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

СКЗИ «КриптоПро CSP» v 4.0 R4 $ $ ' для криптографической защиты персональных данных.

Установочные модули СКЗИ «КриптоПро CSP» v 4.0 R4 и комплект эксплуатационной документации к нему могут поставляться пользователю Уполномоченной организацией двумя способами:

1. На носителе (CD, DVD - диски);
2. Посредством загрузки через Интернет.

Для получения возможности загрузки установочных модулей СКЗИ «КриптоПро CSP» v 4.0 R4 и комплекта эксплуатационной документации пользователь направляет свои учетные данные Уполномоченной организации. Учетные данные могут быть направлены посредством заполнения специализированной регистрационной формы на сайте Уполномоченной организации.

После получения Уполномоченной организацией учетных данных пользователю предоставляется доступ на страницу загрузки установочных модулей СКЗИ «КриптоПро CSP» v 4.0 R4 и комплекта эксплуатационной документации. При загрузке пользователем установочных модулей СКЗИ «КриптоПро CSP» v 4.0 R4 и комплекта эксплуатационной документации Уполномоченной организацией присваивается учетный номер, идентифицирующий экземпляр СКЗИ «КриптоПро CSP» v 4.0 R4, предоставленный пользователю.

На странице загрузки вместе с дистрибутивом и документацией размещается отделенная электронная подпись, для проверки которой необходимо использовать утилиту cpverify, полученную доверенным образом и содержащую ключ проверки данной электронной подписи.

Установка СКЗИ «КриптоПро CSP» v 4.0 R4 на рабочее место пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей СКЗИ «КриптоПро CSP» v 4.0 R4 и эксплуатационной документации.

	1. Средство контроля целостности (cpverify.exe) первоначально должно быть получено пользователем на физическом носителе в офисе компании ООО «КРИПТО-ПРО», либо у официального дилера. Такая утилита считается полученной доверенным образом. Далее полученной доверенным образом признается очередная версия утилиты, полученная любым образом, например, скачанная с сайта www.cryptopro.ru, при условии, что она была проверена другим экземпляром утилиты, полученным ранее доверенным образом, и проверка была успешной. 2. Ключ проверки ЭП, а также информация о нем (дата создания, алгоритм хэш-функции, идентификатор алгоритма подписи) записываются в исходный код утилиты на этапе сборки.

3. Программно-аппаратные среды функционирования СКЗИ

СКЗИ «КриптоПро CSP» v 4.0 R4 функционирует в следующих группах программно-аппаратных сред:

Windows

Включает программно-аппаратные среды:

Windows XP[1] (x86);
Windows 7/8/8.1/10/Server 2003/2008 (x86, x64);
Windows Server 2008 R2/2012/2012 R2/2016 (x64).

LSB Linux

Включает дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360 версии LSB 4.x:

CentOS 4/5/6 (x86, x64);
CentOS 7 (x86, x64, POWER, ARM, ARM64);
ОСь (OS-RT) (x64);
ТД ОС АИС ФССП России (GosLinux) (x86, x64);
Red OS (x86, x64);
Fedora 27/28/29 (x86, x64, ARM);
Oracle Linux 4/5/6 (x86, x64);
Oracle Linux 7 (x64);
OpenSUSE Leap 42, 15 (x86, x64, ARM, ARM64);
AlterOS (x64);
SUSE Linux Enterprise Server 11SP4 (x86, x64);
SUSE Linux Enterprise Server 12/15, Desktop 12/15 (x64, POWER, ARM64);
Red Hat Enterprise Linux 4/5/6 (x86, x64);
Red Hat Enterprise Linux 7 (x64, POWER, ARM64);
Синтез-ОС.РС (x86, x64);
ПК «СинтезМ-Клиент» в составе КП «ЗОС «СинтезМ» (x64);
ПК «СинтезМ-Сервер» в составе КП «ЗОС «СинтезМ» (x64);
КП «ОС «СинтезМ-К» (x64);
Ubuntu 14.04/16.04 (x86, x64, POWER, ARM, ARM64);
Ubuntu 18.04/18.10 (x86, x64);
Linux Mint 17/18/19 (x86, x64);
Debian 7/8/9 (x86, x64, POWER, ARM, ARM64, MIPS);
ОС Лотос (x86, x64);
Astra Linux Special Edition, Common Edition (x64, MIPS, Эльбрус);
МСВСфера 6.3 Сервер (x64, ARM64).

Unix

Включает программно-аппаратные среды:

ОС Эльбрус версия 3 (Эльбрус);
ALT Linux 6/7 (x86, x64, ARM);
Альт Сервер 8, Альт 8 СП Сервер (x86, x64, ARM, ARM64);
Альт Рабочая станция 8, Альт Рабочая станция К 8, Альт 8 СП Рабочая станция (x86, x64, ARM, ARM64);
ROSA Fresh, Enterprise Desktop, Enterprise Linux Server (x86, x64);
РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);
FreeBSD 11, pfSense 2.x (x86, x64);
AIX 6/7 (POWER);
Mac OS X 10.9/10.10/10.11/10.12/10.13/10.14 (x64).

Solaris

Включает программно-аппаратные среды:

Solaris 10 (sparc, x86, x64);
Solaris 11 (sparc, x64).

Sailfish

Включает программно-аппаратную среду

SailfishOS 2.1.1.12 (ARMv7).

iOS

Включает программно-аппаратные среды:

Apple iOS 8.0/8.0.1/8.0.2/8.1/8.1.1/8.1.2/8.1.3/8.2/8.3/8.4/8.4.1/9/9.0.1/9.0.2/9.1/9.2/9.2.1/9.3/9.3.1/9.3.2/9.3.3/9.3.4/9.3.5/10/11/12 (ARMv7, ARM64).

Виртуальные среды

Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016 (x64);
Microsoft Hyper-V 8/8.1/10 (x64);
Citrix XenServer 7 (x64);
VMWare WorkStation 11/12/14/15 (x86, x64);
VMWare WorkStation Player 12/14/15 (x86, x64);
VMWare vSphere ESXi/Hypervisor 5.5/6.0/6.5/6.7 (x64);
Oracle VirtualBox 5.2 (x86, x64);
RHEV 4 (x64).

Примечания:

1. Версия POSReady.

4. Реализуемые криптографические алгоритмы

Алгоритм шифрования/расшифрования данных и вычисления имитовставки реализован в соответствии с требованиями ГОСТ Р 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Алгоритмы формирования и проверки ЭП реализованы в соответствии с требованиями ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

Алгоритм выработки значения хэш-функции реализован в соответствии с требованиями ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».

S-боксы, группы точек на эллиптических кривых, значения функций хэширования определены в документе RFC 4357, Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ), Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Системы обработки информации. Защита криптографическая. Методические рекомендации по криптографическим алгоритмам, сопутствующим применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012».

Ключевая система СКЗИ «КриптоПро CSP» v 4.0 R4 обеспечивает возможность парно-выборочной связи абонентов сети с выработкой для каждого сеанса связи ключей на основе принципа открытого распределения ключей с использованием алгоритма Диффи-Хеллмана.

5. Структура и состав СКЗИ

5.1. Структура СКЗИ

Общая структура СКЗИ представлена на Рисунке 5.1.

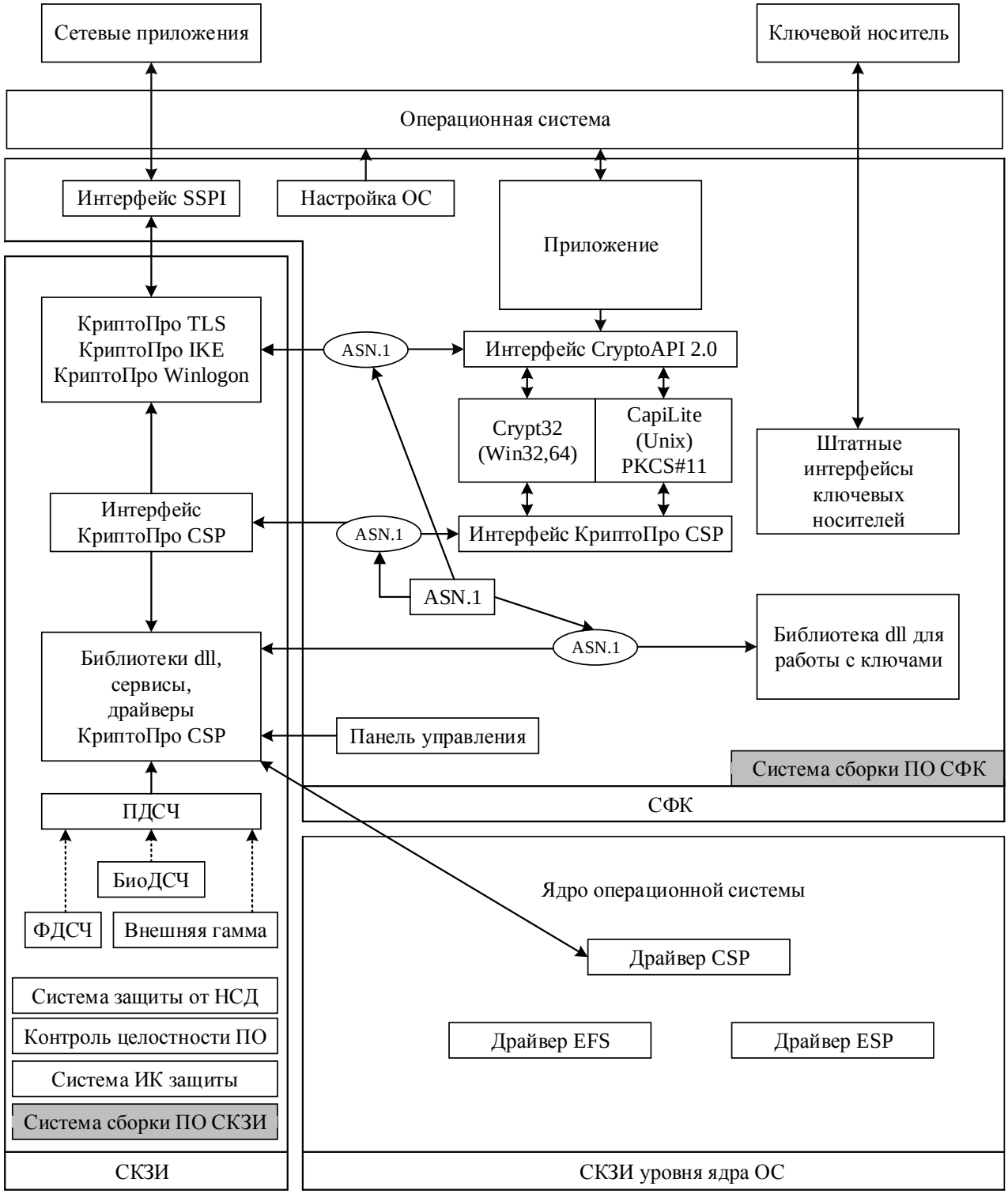


Рисунок 5.1 – Структура СКЗИ «КриптоПро CSP 4.0 R4»

5.2. Состав СКЗИ

Исполнение 1-Base класса защиты КС1 выполнено в следующем составе:

- криптопровайдер;
- криптодрайвер;
- модуль сетевой аутентификации (КриптоПро TLS);
- модуль обработки сертификатов и CMS протокола;
- утилита выработки внешней гаммы;
- утилита командной строки для шифрования файлов;
- утилита командной строки для работы с сертификатами;
- модуль аутентификации пользователя в домене Windows;
- пакет разработчика для использования протоколов IPsec (IPsec SDK);
- пакет разработчика для встраивания СКЗИ (CSP SDK);
- модуль поддержки интерфейса Mozilla NSS;
- сервисные модули (cpverify, wipefile, stunnel);
- библиотека, обеспечивающая подключение и функционирование ключевых носителей (RDK)

и функционирует в группах программно-аппаратных сред п.3.

5.3. Состав программного обеспечения СКЗИ

СКЗИ «КриптоПро CSP» v 4.0 R4 функционирует на одном из двух уровней:

- уровень приложения;
- уровень ядра ОС.

В состав СКЗИ «КриптоПро CSP» v 4.0 R4 входят:

- Библиотеки dll, сервисы, драйверы «КриптоПро CSP».
- Модуль сетевой аутентификации «КриптоПро TLS».
- Модуль «КриптоПро Winlogon».
- Криптографический интерфейс «КриптоПро CSP».
- Программный датчик случайных чисел (ПДСЧ) с инсталляцией от физического ДСЧ (ФДСЧ) встраиваемого программно-аппаратного комплекса (ПАК) защиты от НСД, БиоДСЧ, внешней гаммы.
- Контроль целостности программного обеспечения.
- Система инженерно-криптографической защиты.
- Система защиты от НСД (используется опционально).

5.4. Состав подсистемы программной СФК

В состав подсистемы программной СФК входят следующие компоненты:

- Приложение (Прикладное программное обеспечение, использующее СКЗИ).
- Интерфейс SSPI (подмножество интерфейса криптографических протоколов Secure Support Provider Interface (SSPI, CryptoAPI v. 2.0) для реализации протокола сетевой аутентификации TLS v. 1.0 (под управлением ОС Windows).
- Модули настройки ОС Windows для обеспечения функционирования СКЗИ.

– Интерфейс CryptoAPI 2.0.

– Средства Crypt32(Win32,64) для обеспечения работы с сертификатами с использованием интерфейса CryptoAPI 2.0 через криптографический интерфейс «КриптоПро CSP» под управлением ОС Windows.

– Средства CapiLite - для обеспечения работы с сертификатами с использованием интерфейса CryptoAPI 2.0 через криптографический интерфейс «КриптоПро CSP» под управлением ОС семейства UNIX (Linux , FreeBSD, Solaris, AIX).

– Криптографический интерфейс «КриптоПро CSP».

– Штатные интерфейсы ключевых носителей.

– ASN.1 - система кодирования/декодирования данных в форматах ASN.1.

Состав модулей СКЗИ и подсистемы программной СФК для соответствующих программно-аппаратных сред конкретизируется в дополнениях ЖТЯИ.00087-03 91 02, ЖТЯИ.00087-03 91 03, ЖТЯИ.00087-03 91 04, ЖТЯИ.00087-03 91 05, ЖТЯИ.00087-03 91 06, ЖТЯИ.00087-03 91 07, ЖТЯИ.00087-03 91 08, ЖТЯИ.00087-03 91 09, ЖТЯИ.00087-03 91 10 к настоящему документу.

5.5. Получение прав на использование СКЗИ «КриптоПро CSP»

При использовании СКЗИ «КриптоПро CSP» версия 4.0 R4 допускаются следующие способы получения подтверждения права использовать СКЗИ «КриптоПро CSP» версия 4.0 R4:

1. Ручной ввод лицензионных данных.

2. Получение данных из соответствующих расширений сертификатов ключей проверки электронной подписи в ключевом контейнере. Таким образом может передаваться право на использование СКЗИ «КриптоПро CSP» версия 4.0 R4 при операциях с соответствующим ключом электронной подписи в рамках срока его действия.

Порядок действий, необходимых для ручного ввода лицензии, зависит от используемой платформы и подробно описан в соответствующих документах: ЖТЯИ.00087-03 92 01, ЖТЯИ.00087-03 91 03, ЖТЯИ.00087-03 91 04, ЖТЯИ.00087-03 91 05, ЖТЯИ.00087-03 91 06, ЖТЯИ.00087-03 91 07, ЖТЯИ.00087-03 92 02, ЖТЯИ.00087-03 91 09.

Ключевая система и ключевые носители

5.6. Общие положения

СКЗИ «КриптоПро CSP» v 4.0 R4 является системой с открытым распределением ключей на основе асимметричной криптографии с использованием закрытого ключа на одной стороне и соответствующего ему открытого ключа информационного взаимодействия на другой стороне.

Пользователь, обладающий правом подписи и/или шифрования данных, вырабатывает на своем рабочем месте или получает у администратора безопасности (в зависимости от принятой политики безопасности) личные закрытый ключ (ключ ЭП) и открытый ключ (ключ проверки ЭП). На основе каждого открытого ключа (ключа проверки ЭП) Удостоверяющим Центром формируется сертификат открытого ключа (сертификат ключа проверки ЭП).

5.6.1. Шифрование данных

При зашифровании сообщения пользователем А для пользователя Б, пользователь А формирует симметричный ключ связи (сеансовый ключ информационного обмена) на основе своего закрытого ключа обмена и открытого ключа обмена пользователя Б. Соответственно, для расшифрования этого сообщения пользователем Б формируется тот же симметричный ключ на основе своего закрытого ключа обмена и открытого ключа обмена пользователя А.

Таким образом, для обмена данными каждому пользователю необходимо иметь:

– личный закрытый ключ обмена;

– открытые ключи обмена других пользователей.

Сеансовый ключ информационного обмена вырабатывается на основе алгоритма Диффи-Хеллмана. Алгоритм Диффи-Хеллмана обеспечивает формирование сеансовых ключей, но не обеспечивает аутентификацию связывающихся сторон. Поэтому данный алгоритм должен использоваться совместно с протоколами аутентификации, в частности, с протоколом «КриптоПро IKE».

5.6.2. Формирование и проверка ЭП

Для формирования электронной подписи используется ключ электронной подписи, для проверки – соответствующий ключ проверки электронной подписи. Проверяющий должен быть полностью уверен в принадлежности ключа проверки ЭП конкретному пользователю. Для этой цели используется сертификат ключа проверки ЭП, подписанный Удостоверяющим Центром.

Каждому пользователю, обладающему правом подписи, необходимо иметь:

– ключ электронной подписи;

– ключи проверки электронной подписи (сертификаты ключей проверки электронной подписи) других пользователей.

ò & % # $ $ $ ' '
÷

ï # # & # $ $ ' ' &
' $ ' ' ÷

5.7. Ключевой контейнер

Закрытые ключи СКЗИ «КриптоПро CSP» v 4.0 R4 хранятся в ключевом контейнере, который может содержать в себе:

– только ключ подписи;

– только ключ обмена;

– ключ подписи и ключ обмена одновременно.

Единственный ключ ключевого контейнера (ключ подписи или ключ обмена) называется первичным ключом. Если в контейнере два ключа, то первый ключ - ключ подписи - называется первичным, второй ключ – ключ обмена - вторичным.

Ключевой контейнер содержит кроме ключей служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности и т.п.

Каждый ключевой контейнер (независимо от типа носителя), является самодостаточным и содержит всю необходимую информацию для работы как с самим контейнером, так и с закрытыми (и соответствующими им открытыми) ключами.

На ключевом носителе ключи хранятся в формате ключевого контейнера.

5.8. Формат ключевого контейнера

Ключевой контейнер содержит следующую информацию:

- первичный ключ;
- маски первичного ключа;
- контрольную информацию первичного ключа;
- вторичный ключ (опциональный);
- резервную копию ключевого контейнера.

Каждый закрытый ключ хранится в формате, дополнительно содержащем все константы, необходимые для формирования и экспорта открытого ключа.

Формат ключевого контейнера обеспечивает чтение ключей и соответствующих масок отдельными операциями в раздельные (разнесенные по адресам) области памяти, для чего он содержит шесть зон (реализация зон зависит от типа ключевого носителя).

Ключевой контейнер содержит также дополнительную информацию, необходимую для обеспечения его восстановления при возникновении различных программно-аппаратных сбоев (дополнительная информация включается в тех случаях, когда размер ключевого контейнера не ограничен размерами памяти физического носителя).

Для использования ключевого контейнера только на одном определенном ПК (например, для привязки токена к ПК), возможно этот контейнер зашифровать на другом контейнере, хранящимся на этом ПК (желательно не экспортируемом).

5.9. Формирование ключей

Формирование ключей пользователя производится с использованием функции CPGenKey (см. ЖТЯИ.00087-03 96 01. КриптоПро CSP. Руководство программиста) и спецификацией типа формируемого ключа: AT_KEYEXCHANGE. AT_SIGNATURE, AT_UECSYMMETRICKEY.

Формирование ключей возможно, если:

1. контекст криптопровайдера «КриптоПро CSP» открыт функцией CPAcquireContext с флагом CRYPT_NEWKEYSET и несуществующим именем ключевого контейнера, специфицированным параметром pszContainer;

2. контекст криптопровайдера «КриптоПро CSP» открыт функцией CPAcquireContext с указанием ранее созданного ключевого контейнера, специфицированного параметром pszContainer.

1. Для исполнения 1-Base закрытые ключи ЭП и обмена формируются с использованием ПДСЧ с инициализацией его от БиоДСЧ или от внешней гаммы.

2. При использовании считывателей смарт-карт или устройств чтения таблеток Touch-Memory DALLAS необходимо проведение проверки настройки используемых ими портов ПЭВМ в BIOS и ОС.

3. Перед использованием процессорные карты должны быть «выпущены» с использованием транспортного пин-кода и ПО выпуска карт (поставляются дистрибутором карт)

4. При использовании НГМД в качестве ключевого носителя во избежание потери ключевой информации рекомендуется хранить ее копию.

В связи с переходом на использование алгоритма ГОСТ Р 34.10-2012 [30] и соответствующем запрете использования алгоритма ГОСТ Р 34.10-2001, при попытке генерации ключа алгоритма ГОСТ Р 34.10-2001 после 01 июня 2018 года будет выдано следующее предупреждение:

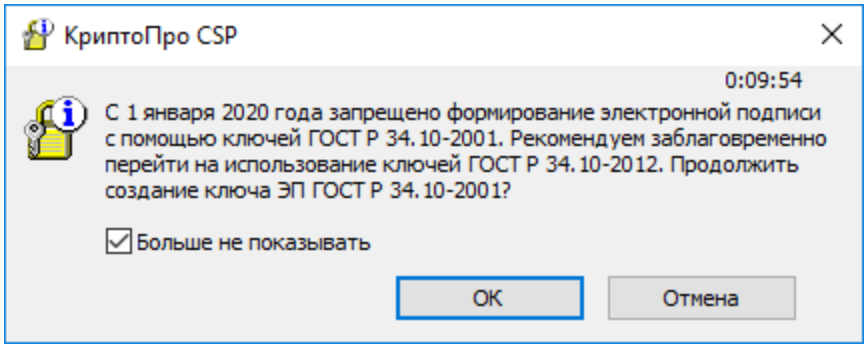


Рисунок 6.1 – Предупреждение о генерации ключа для ОС семейства Windows

Примечание: на других операционных системах окно внешне может выглядеть по-другому, но текстовая составляющая аналогична приведенной на рисунке.

При выборе «Больше не показывать» предупреждения о генерации ключа и создании подписи будут отложены до 01 января 2020 года. При повторном выборе «Больше не показывать» предупреждения более появляться не будут.

При попытке создания подписи с использованием ключа алгоритма ГОСТ Р 34.10-2001 после 01 июня 2018 года будет выдано следующее предупреждение.

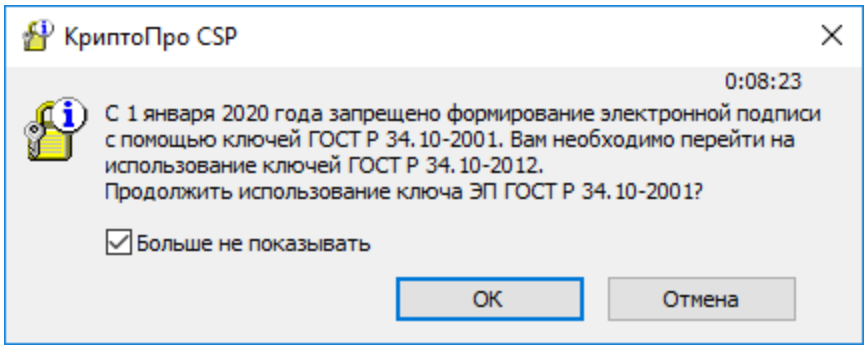


Рисунок 6.2 – Предупреждение о создании подписи для ОС семейства Windows

Примечание: на других операционных системах окно внешне может выглядеть по-другому, но текстовая составляющая аналогична приведенной на рисунке.

При выборе «Больше не показывать» предупреждение о создании подписи будет отложено до 01 января 2020 года. При повторном выборе «Больше не показывать» предупреждение более появляться не будет.

Создание подписи с использованием ключа алгоритма ГОСТ Р 34.10-2001 с 01 января 2020 года запрещено.

5.10. Ключевые носители

В качестве ключевых носителей используются:

- ГМД 3,5”, USB диски;
- Смарткарты GEMALTO (GemSim1, GemSim2, Optelio, OptelioCL, OptelioCL2, Native);
- eToken, Jacarta;

- USB-токены Рутокен ЭЦП (Flash, Bluetooth), Рутокен Lite Novacard;
- Смарткарты Рутокен Lite SC, Рутокен ЭЦП SC;
- Rutoken S;
- Смарткарты РИК (ОСКАР 1, ОСКАР 2, Магистра, TRUST, TRUSTS, TRUSTD);
- Смарткарта УЭК;
- Смарткарта MS_KEY K;
- Токен++ Lite;
- ESMART Token;
- Смарткарты Athena IDProtect, MorphoKST, Cha cardOS, Cha JCOP;
- Смарткарты Алиот INPASPOT Series, SCOne Series;
- Rosan;
- Раздел HDD ПЭВМ (в Windows - реестр);
- Идентификаторы Touch-Memory DS1995, DS1996.

Использование ключевых носителей в зависимости от программно-аппаратной платформы отражено в ЖТЯИ.00087-03 30 01. КриптоПро CSP. Формуляр, п. 3.8.

	1. В состав дистрибутива СКЗИ входят библиотеки поддержки всех перечисленных носителей, но не входят драйверы для ОС. По вопросам получения драйверов необходимо обращаться к производителям соответствующих устройств. 2. Хранение закрытых ключей на HDD ПЭВМ и USB дисках (в реестре ОС Windows, в разделе HDD при работе под управлением других ОС) допускается только при условии распространения на HDD, USB диск или на ПЭВМ с HDD требований по обращению с ключевыми носителями (п.6.7 ЖТЯИ.00087-03 91 01. Руководство администратора безопасности общая часть). 3. Все вышеперечисленные носители используются только в качестве пассивного хранилища ключевой информации без использования криптографических механизмов, реализованных на смарт-карте/токене. 4. Использование носителей других типов - только по согласованию с ФСБ России.

5.11. Размеры ключей

Длины ключей электронной подписи:

ключ электронной подписи	256 или 512 бит;
ключ проверки электронной подписи	512 или 1024 бит.

Длины ключей, используемых при шифровании:

закрытый ключ	256 бит или 512 бит;
открытый ключ	512 бит или 1024 бита;
симметричный ключ	256 бит.

5.12. Хранение ключевых носителей

При хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Пользователь несет персональную ответственность за хранение личных ключевых носителей.

Запрещается оставлять без контроля вычислительные средства с установленным СКЗИ после ввода ключевой информации.

В случае централизованного хранения ключевых носителей в организации, эксплуатирующей СКЗИ, администратор безопасности (если он имеется) несет персональную ответственность за хранение личных ключевых носителей пользователей.

При хранении ключей в реестре Windows и на HDD ПЭВМ требования по хранению личных ключевых носителей распространяются на ПЭВМ (HDD ПЭВМ) (в том числе и после удаления ключей из реестра, из HDD).

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

При хранении ключей на HDD ПЭВМ необходимо использовать парольную защиту.

СКЗИ может функционировать и хранить ключевую информацию в двух режимах:

– в памяти приложения;

– в «Службе хранения ключей», реализованной в виде системного сервиса.

Ключи находятся в кэше до завершения приложения или до выключения компьютера (остановки службы), что позволяет использовать закрытый ключ даже после закрытия криптографического контекста.

Функционирование и хранение ключей СКЗИ «КриптоПро CSP». v 4.0 R4 в «Службе хранения ключей» обеспечивает дополнительную защиту ключевой информации от других приложений, выполняющихся на ПЭВМ, но может незначительно замедлить производительность системы.

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

5.13. Сроки действия пользовательских ключей

При эксплуатации СКЗИ «КриптоПро CSP». v 4.0 R4 должны соблюдаться следующие сроки использования пользовательских закрытых ключей и сертификатов:

– максимальный срок действия закрытого ключа ЭП-256 (ключа ЭП) - 1 год 3 месяца;
– максимальный срок действия закрытого ключа ЭП-512 (ключа ЭП) - 1 год 3 месяца;
– максимальный срок действия открытого ключа ЭП-256 (ключа проверки ЭП) - 15 лет;
– максимальный срок действия открытого ключа ЭП-512 (ключа проверки ЭП) - 15 лет;
– максимальный срок действия закрытых и открытых ключей обмена – 1 год 3 месяца.

При формировании закрытого ключа в контейнер записывается дата истечения срока действия этого ключа, по истечении которого в зависимости от значения параметра ControlKeyTimeValidity возможны различные варианты использования этого ключа.

Значение «0» параметра не накладывает никаких ограничений на использование ключа.

Значение «1» параметра запрещает формирование ЭП и шифрование в контексте этого ключа (возможно расшифрование ранее зашифрованных сообщений) (значение по умолчанию);

Значение «2» параметра запрещает любые действия с закрытым ключом.

Срок действия ключа берется из (в порядке уменьшения приоритета):

– Расширения контейнера ключа;
– Расширения сертификата ключа;
– Даты создания ключа + 1 год 3 месяца.

Изменение параметра ControlKeyTimeValidity

Для операционных систем группы Windows необходимо изменить значение ключа реестра
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Crypto Pro\Cryptography\CurrentVersion\Parameters\ControlKeyTimeValidity (для 64-битных операционных систем),
HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\Parameters\ControlKeyTimeValidity (для 32-битных операционных систем).

Настройка СКЗИ для остальных ОС осуществляется с помощью утилиты cpconfig с помощью команды

```
./cpconfig -ini '\config\parameters' -add long ControlKeyTimeValidity <значение>
```

	При работе в режиме усиленного контроля использования ключей (режим обязателен к использованию, отключение может производиться только в целях тестирования) значение параметра ControlKeyTimeValidity принимается равным «2».

5.14. Уничтожение ключей на ключевых носителях

Ключи на ключевых носителях (включая Touch Memory и смарт-карты), срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

Об уничтожении ключей делается соответствующая запись в «Журнале пользователя сети» (см. Ведение журналов п.8.11).

5.15. Интерфейс управления ключами СКЗИ

Последовательность действий при генерации закрытых ключей и ключей ЭП пользователей, управлении их паролями, управлении ключами определена в документе «ЖТЯИ.00087-03 92 01. КриптоПро CSP. Инструкция по использованию СКЗИ под управлением ОС Windows».

6. Протокол сетевой аутентификации «КриптоПро TLS»

Модуль поддержки сетевой аутентификации позволяет реализовать защищенный сетевой протокол в соответствии с рекомендациями RFC 2246 «The TLS Protocol. Version 1.0» и «Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)». Модуль обеспечивает двустороннюю и одностороннюю аутентификацию приложений при их взаимодействии по сети с использованием алгоритма ЭП и сертификатов открытых ключей, а также шифрование данных, передаваемых в сетевом соединении.

Прикладное программное обеспечение может использовать протокол TLS для аутентификации и защиты данных, передаваемых по собственным протоколам на основе TCP/IP и HTTPS.

Протокол TLS (Transport Layer Security, спецификация IETF - RFC2246) относится к средствам защиты прикладных пакетов Microsoft Internet Explorer/Microsoft Edge, Internet Information Services (IIS), Microsoft SQL Server 2000 и COM+. Он обеспечивает аутентификацию связывающихся сторон, конфиденциальность и целостность пересылаемой информации. Аутентификация обеспечивается использованием сертификатов стандарта X.509 (в средах с сильной аутентификацией), конфиденциальность – шифрованием пересылаемых данных, целостность — применением хэш-функции и кода аутентификации сообщения (Message Authenticity Code, MAC).

Для подключения по протоколу TLS используется префикс https, при этом обозреватель Web-сервера по умолчанию будет подключаться к порту TCP 443 вместо стандартного порта TCP 80. Если сервер не поддерживает протокол TLS, соединение не устанавливается. Применение протоколов SSL/TLS (SSL - более ранние версии протокола) показано в Таблице 7.1.

Таблице 7.1 – Применение протоколов SSL/TLS.

÷	÷	ö
HTTPS	443	HTTP по SSL/TLS
SMTPS	465	SMTP (электронная почта) по SSL/TLS
NNTPS	563	NNTP (новости) по SSL/TLS
LDAPS	636	LDAP (доступ к каталогам) по SSL/TLS
POP3S	995	POP (электронная почта) по SSL/TLS
IRCS	994	IRC по SSL/TLS
IMAPS	993	IMAP (электронная почта) по SSL/TLS
FTPS	990	FTP (передача файлов) по SSL/TLS

Для того, чтобы протокол SSL/TLS действовал, Web-сервер должен иметь пару сертификат открытого ключа/закрытый ключ. Владелец сертификата должен подтвердить, что он является владельцем закрытого ключа, связанного с сертификатом. Это дает возможность клиенту аутентифицировать сервер, с которым он хочет связаться.

В процессе взаимной аутентификации:

– выполняется криптографическая проверка наличия у сервера закрытого ключа, соответствующего открытому ключу, указанному в сертификате;

– проверяется степень доверия издателю сертификата;

– проверяется, не истек ли срок действия сертификата;

– проверяется, не отозван ли сертификат; по умолчанию Internet Explorer/Microsoft Edge эту проверку не выполняет — это делает IIS.

Если любая из указанных проверок приводит к отрицательному результату, пользователь получает предупреждение и может разорвать соединение (это рекомендуется сделать).

Достигнув доверия, стороны вырабатывают сеансовый ключ, на основе которого обеспечивается шифрование данных в течение сеанса.

6.1. Основные понятия протокола TLS

Протокол TLS предназначен для обеспечения криптографическими средствами аутентификации отправителя (клиента) и адресата (сервера), контроля целостности и шифрования данных информационного обмена.

Аутентификация опционально может быть односторонней (аутентификация сервера клиентом), взаимной (встречная аутентификация сервера и клиента) или не использоваться.

Иерархия информационного обмена включает в себя сессии, соединения и поток сообщений в соединении. Поток сообщений при большой длине разбивается на фрагменты с пакетной передачей фрагментов. В одной сессии может быть реализовано несколько соединений, произвольно разнесенных по времени. В каждом соединении может быть обработан необходимый поток сообщений.

Сессия характеризуется следующими атрибутами:

– идентификатор сессии (случайное число, 32 байта, задается сервером при открытии сессии);

– метод компрессии;

– сертификат сервера (опционально);

– сертификат клиента (опционально);

– спецификация алгоритмов и параметров защиты (алгоритмы шифрования и MAC, криптографические параметры);

– master secret (используется при генерации ключей шифрования, ключей MAC, векторов инициализации);

– флаг, разрешающий/запрещающий новые соединения в сеансе.

Сертификаты представляются в стандарте X509. v3. Спецификация алгоритмов и параметров защиты может меняться в течение сессии.

Соединение характеризуется следующими атрибутами:

– client_random – случайные 32 байта, задаваемые клиентом;

– server_random– случайные 32 байта, задаваемые сервером;

– client write MAC secret (ключ клиента для вычисления значения ключевой хэш–функции);

– server write MAC secret (ключ сервера для вычисления значения ключевой хэш–функции);

– client write key (ключ, используемый для шифрования данных клиентом и расшифрования их сервером);

– server write key (ключ, используемый для шифрования данных сервером и расшифрования их клиентом);

– client write IV, server write IV (векторы инициализации, используемые клиентом и сервером соответственно);

– порядковый номер соединения (поддерживается независимо для передаваемых и принимаемых сообщений).

Вектор инициализации задается для первого фрагмента сообщения в соединении; для последующих фрагментов вектор инициализации формируется из конечного блока зашифрованного текста предыдущего фрагмента.

Порядковые номера соединений поддерживаются независимо для передаваемых и принимаемых сообщений. При смене сессии, изменении спецификации алгоритмов и параметров защиты нумерация соединений начинается с 0; Диапазон нумерации: 0 ÷ 264-1.

Соединение ассоциируется с одной сессией.

Алгоритм преобразования информации при обмене с использованием протокола TLS включает следующие операции:

– прием от протокола верхнего уровня потока не интерпретируемых данных в блоках произвольного размера;

– фрагментация принятых с верхнего уровня данных в структурированные блоки (фрагменты) протокола TLS. Размер фрагмента – не более 2^{14} байт;

– компрессия фрагментов (опционально);

– вычисление значения ключевой хэш-функции (MAC) от конкатенации ключа хэш-функции, типа компрессии, длины компрессированного фрагмента, компрессированного фрагмента и заданной константы;

– конкатенация фрагмента и результата вычисления значения хэш-функции от него (расширенный фрагмент);

– зашифрование расширенного фрагмента (опционально);

– добавление открытого заголовка, содержащего тип сообщения (один байт), версию протокола TLS (два байта) и длину компрессированного фрагмента.

При приеме информации применяется обратная последовательность операций.

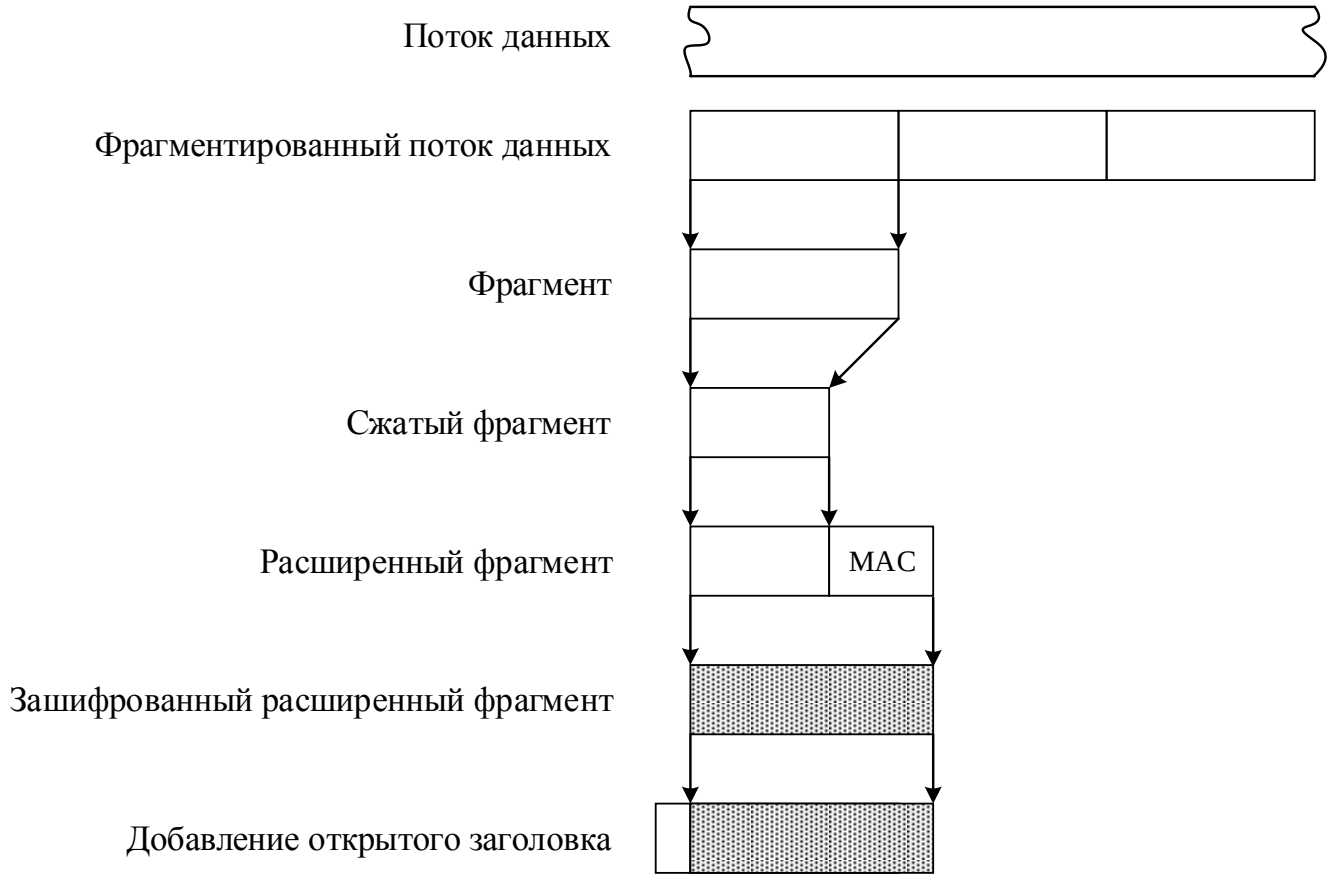


Рисунок 7.1 — Алгоритм преобразования информации при обмене с использованием протокола TLS

В протоколе TLS используются следующие типы сообщений:

– Hello message (ClientHello, ServerHello);

– Change cipher specs message (изменение спецификации алгоритмов и параметров защиты);

– Key exchange message (передача ключа обмена ключами шифрования и MAC клиента, сервера);

– Alert message (предупреждение, оповещение о фатальной ошибке);

– Application_data message (передача данных);

– Finished message (сообщение о возможности работы в созданной сессии).

Протокол TLS является двухуровневым и действует над транспортным протоколом. К первому уровню относятся TLS Handshake Protocol, TLS Change Cipher Spec и TLS Alert Protocol. Ко второму уровню относится TLS Record Protocol.

TLS Handshake Protocol обеспечивает инициализацию сессии (соединения) выполнением следующих операций:

– клиент и сервер договариваются об используемых в сессии алгоритмах и параметрах защиты, обмениваются случайными величинами client_random, server_random, договариваются, будут или нет новые соединения;

– производится обмен сертификатами для аутентификации клиента и сервера (по заданным опциям);

– клиент генерирует случайную величину pre_master secret, шифрует ее и передает серверу.

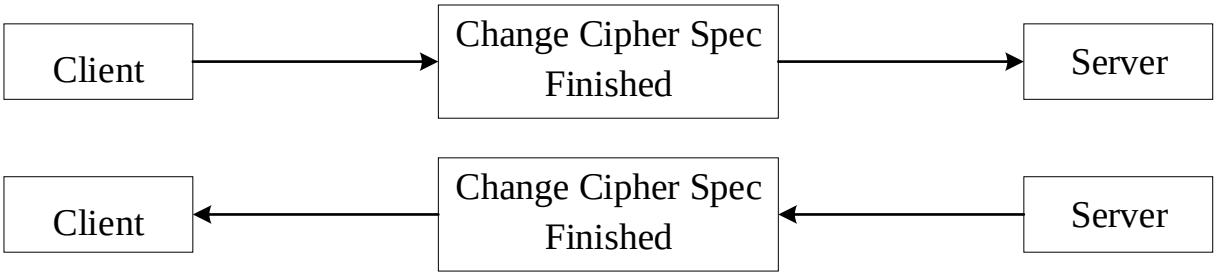
– клиент и сервер по pre_master secret, client_random и server_random формируют master secret (набор необходимой ключевой информации) сессии.

TLS Handshake Protocol работает по следующей схеме, представленной на Рисунке 7.2.

Установка версии протокола, идентификатора сессии, начального набора алгоритмов и параметров, метода компрессии.

Сервер посылает (опционально) свой сертификат и запрашивает (опционально) сертификат клиента, передача случайной величины server-random.

Клиент посылает свой сертификат (если был запрос сервера) Если сертификата у клиента нет, он посылает Certificate Verify.



Выбор алгоритмов и параметров для устанавливаемой сессии, завершение Handshake («рукопожатия»).

Рисунок 7.2 – Схема работы TLS Handshake Protocol.

6.2. Модуль сетевой аутентификации «КриптоПро TLS»

Модуль сетевой аутентификации «КриптоПро TLS» реализован на базе протокола TLS v.1.0 и российских стандартов криптографической защиты конфиденциальной информации (алгоритмы шифрования в соответствии с ГОСТ 28147-89, алгоритмы выработки и проверки электронной подписи в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, алгоритмы хэширования в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012). Используется также алгоритм Диффи-Хеллмана открытого распределения ключей на базе ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.

Аутентификация клиент-сервер может быть односторонней и двусторонней.

Односторонняя аутентификация обеспечивает минимально необходимый уровень защиты, и включает в себя:

– обязательную аутентификацию сервера без аутентификации клиентов;

– шифрование трафика между клиентом и сервером.

При работе в данном режиме сервер на этапе «рукопожатия» не запрашивает сертификат клиента и устанавливается «анонимное» защищенное соединение. В этом случае клиент может не иметь закрытого ключа и на значок «замка»., однако при этом он лишается возможности формировать электронную подпись под документами. Режим с односторонней аутентификацией сервера может использоваться для предоставления некоторой группе пользователей конфиденциальной информации на основании парольной защиты, однако пароль в этом случае будет предъявляться пользователем только после установления защищенного TLS-соединения с Web-сервером, что повышает уровень защиты от несанкционированного доступа по сравнению с передачей пароля по открытым соединениям. При односторонней аутентификации сервер запрашивает сертификат клиента, но его отсутствие не считается ошибкой.

Двусторонняя аутентификация включает в себя:

– взаимную аутентификацию клиента и Web-сервера с помощью их сертификатов;

– шифрование трафика между клиентом и сервером;

– формирование и проверку электронной подписи под электронными HTML-формами, заполняемыми пользователями.

Двусторонняя аутентификация позволяет обеспечить доступ в закрытую часть Web–сервера только зарегистрированным владельцам сертификатов. При этом нужно иметь в виду, что разграничение доступа к информационным ресурсам сервера, основанное на проверке сертификатов клиентов, гораздо надежнее, чем просто парольная защита.

В данном режиме работы клиенту необходимо сгенерировать закрытый и открытый ключи и получить сертификат открытого ключа в УЦ.

Требования к техническим и программным средствам компьютера, на который устанавливается ISA сервер, определяются в документации, поставляемой вместе с данным сервером. Дополнительно, на компьютер должны быть установлены СКЗИ «КриптоПро CSP» и модуль поддержки сетевой аутентификации «КриптоПро TLS».

Для возможности установления защищенного соединения между клиентом и сервером ISA необходимо вначале выпустить сертификат открытого ключа, который будет использоваться для серверной аутентификации по протоколу TLS.

К такому сертификату предъявляются следующие требования:

– имя сертификата (Common name) должно совпадать с именем публикуемого Web-сервера прикладной системы. Например: pif.nikoil.ru;

– область использования ключа должна содержать: «Аутентификация Сервера».

Данный сертификат должен быть установлен на сервер ISA в привязке с ключом подписи (закрытым ключом). При этом закрытый ключ подписи должен быть помещен в реестр ОС.

Выпуск и установка сертификата осуществляются через АРМ пользователя Центра регистрации. Порядок действий определяется в инструкции пользователю.

6.3. Проверка использования российских алгоритмов в браузере Internet Explorer/Edge.

1. Откройте браузер Internet Explorer/Edge.

При посещении веб-страницы обратите внимание, используется ли протокол соединения «https».

Рисунок 7.3 – Адресная строка Internet Explorer.

2. Нажмите на значок «замка».

Рисунок 7.4 – Адресная строка Internet Explorer.

Должно появится окно следующего вида:

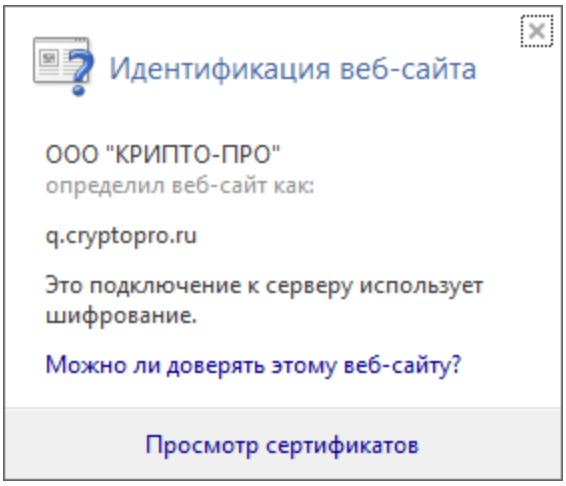


Рисунок 7.5 – Окно идентификации Веб-сайта.

3. Нажмите на Просмотр сертификатов.

Откроется SSL сертификат web-сервера. На вкладке «Состав» можно посмотреть информацию об используемых криптографических алгоритмах.

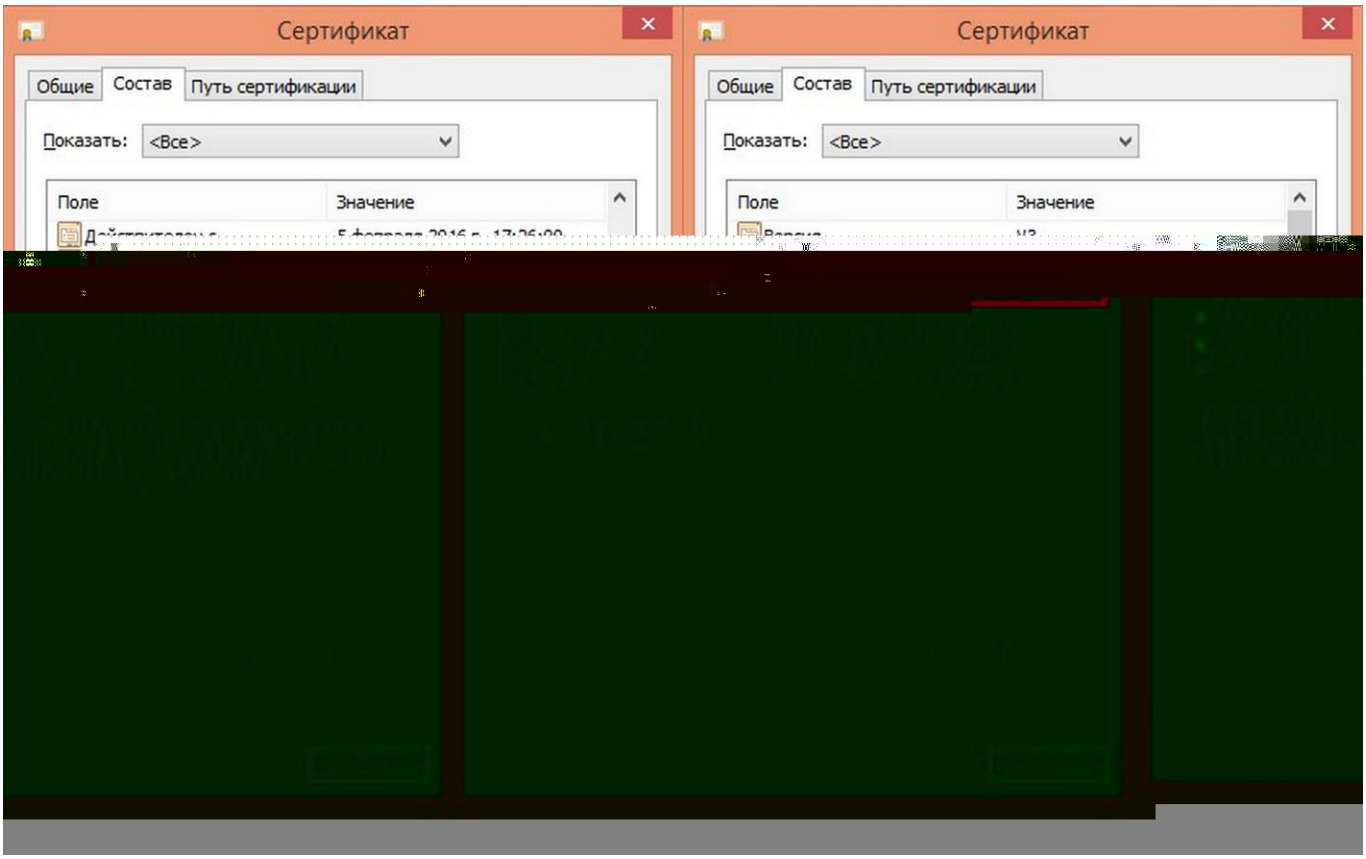


Рисунок 7.6 – Сертификат.

7. Управление ключами СКЗИ

Ключевая система СКЗИ «КриптоПро CSP» v 4.0 R4 базируется на архитектуре PKI рекомендаций X.509. В качестве УЦ может выступать Удостоверяющий центр «КриптоПро УЦ», но допускается использование Центра Сертификации корпорации Microsoft (Microsoft Certification Authority), или другие сертифицированные ФСБ России реализации, обеспечивающие выполнение функций доверенного обращения с сертификатами.

Рекомендации по управлению ключами приведены для «КриптоПро УЦ» с организационной структурой, элементами которой являются:

1. Центр сертификации (ЦС);
2. Центр регистрации (ЦР);
3. АРМ администратора УЦ;
4. Пользовательские средства взаимодействия с УЦ;
5. Программный интерфейс взаимодействия с УЦ.

Описание Удостоверяющего центра «КриптоПро УЦ» приведено в Приложении 4.

	СКЗИ «КриптоПро CSP» v 4.0 R4 может использоваться в качестве криптоядра в составе различных прикладных систем, организационные схемы управления ключевой системой которых могут отличаться от рассматриваемой.

Сертификат открытого ключа обмена и сертификат ключа проверки ЭП представляет собой структурированную двоичную запись в формате ASN.1, содержащую:

– имя субъекта или объекта системы, однозначно идентифицирующее его в системе;

– открытый ключ или ключ проверки ЭП субъекта или объекта системы;

– дополнительные атрибуты, определяемые требованиями использования сертификата в системе;

– ЭП Издателя (Удостоверяющего центра), заверяющую совокупность этих данных.

Формат сертификата определен в рекомендациях ITU-T 1997 года X.509 и рекомендациях IETF 1999 года RFC 2459. В настоящее время основным принятым форматом является формат версии 3, позволяющий определить дополнения (**extensions**), с помощью которых реализуется определенная политика безопасности в системе.

Ниже приведены требования по управлению ключевой системой на всех этапах ее жизненного цикла, начиная с формирования ключей Центра Сертификации. Требования приведены с учетом наличия Центра Регистрации, являющегося функциональной единицей системы. В случае его отсутствия функции Центра Регистрации выполняет Центр Сертификации, функции администратора ЦР выполняет администратор ЦС.

7.1. Удостоверяющий центр

Удостоверяющий центр обеспечивает выполнение следующих функций:

– регистрация (формирование) дистрибутивов ПО СКЗИ и выдача их пользователям;

– формирование, хранение и использование закрытого ключа (ключей) Центра Сертификации;

– регистрация пользователей в соответствии с требованиями Регламента (Договора) системы;

– получение от пользователя запроса на сертификат, как в электронном, так и в бумажном виде;

– верификация запроса на сертификат;

– формирование сертификатов открытых ключей и ключей проверки ЭП пользователей на основе полученных запросов и зарегистрированной информации;

– доставка сертификатов открытых ключей и ключей проверки ЭП пользователям;

– получение и обработка сообщений о компрометации ключей пользователями;

– организация схемы оперативного оповещения пользователей обо всех изменениях, происходящих в сети (компрометация ключей, восстановление конфиденциальной связи после компрометации ключей, включение новых пользователей, плановая смена ключей и т. п.);

– плановое изготовление списка отозванных сертификатов;

– разработка и поддержка функционирования парольной системы оповещения в сети;

– управление ключевой системой;

– разбор конфликтных ситуаций и доказательство авторства электронного документа, снабженного электронной подписью.

– В состав УЦ входят:

– программно-аппаратные средства Центра Сертификации;

– программно-аппаратные средства Центра Регистрации (при условии его эксплуатации на отдельной ПЭВМ);

– программно-аппаратные средства для разбора конфликтных ситуаций;

– дополнительные средства, обеспечивающие сетевое взаимодействие пользователей и УЦ.

7.2. Формирование ключей Центра Сертификации

Формирование ключей Центра Сертификации производится администратором ЦС следующим образом:

1. Администратор ЦС регистрируется в УЦ в «Журнале регистрации администраторов безопасности и пользователей» (см. 7.11 «Ведение журналов»). Регистрацию проводит начальник УЦ (о чем делается соответствующая отметка в журнале).

2. Администратор ЦС производит формирование закрытого ключа ЦС и сертификата открытого ключа ЦС. С закрытого ключа ЦС формируется резервная копия, которая хранится у начальника УЦ. Факт изготовления ключа и сертификата ЦС заносится в «Журнале пользователя сети» и заверяется начальником УЦ.

3. Бланк сертификата ЦС выводится на принтер в двух экземплярах и заверяется начальником УЦ и администратором ЦС. Одна копия бланка сертификата ЦС хранится у начальника УЦ, вторая копия передается администратору ЦР (ЦС).

4. Администратор ЦС производит формирование СОС ЦС, который не содержит ни одного отозванного сертификата. Бланк СОС выводится на принтер в двух экземплярах и заверяется администратором ЦС. Одна копия бланка СОС ЦС хранится и начальника УЦ, вторая копия передается администратору ЦР (ЦС).

	При формировании СОС ЦС и наличии сетевых средств распространения СОС в системе, рекомендуется установить в СОС дополнение «Точка распространения СОС» (issuingDistributionPoint) с заданием в нем метода доступа, который может быть использован пользователями для регулярного обновления СОС (см. [25]).

7.3. Хранение и использование закрытого ключа ЦС

Закрытый ключ ЦС и его резервная копия хранятся у начальника УЦ. При необходимости его использования или в начале рабочего дня (смены, при сменной работе), закрытый ключ ЦС выдается администратору ЦС, о чем делается пометка в «Журнале пользователя сети». Рекомендуется не загружать программное обеспечение ЦС без необходимости, а при загруженном ПО, не оставлять закрытый ключ ЦС без контроля администратора ЦС.

Срок действия закрытого ключа ЦС (точнее, ключа Уполномоченного лица УЦ) составляет 3 года. В течение 1 года 3 месяцев закрытый ключ Уполномоченного лица УЦ используется для изготовления сертификатов пользователей и формирования списков отозванных сертификатов.

По истечении 1 года 3 месяцев и до окончания срока действия закрытого ключа Уполномоченного лица УЦ данный закрытый ключ используется исключительно для формирования списков отозванных сертификатов УЦ.

7.4. Формирование ключей Центра Регистрации

Рекомендации, описанные в данном разделе, относятся только к системам, использующим Центр Регистрации.

7.4.1. Регистрация Центра Регистрации

Администратор ЦС производит регистрацию ЦР в Центре Сертификации, о чем делается запись в «Журнале регистрации администраторов безопасности и пользователей».

7.4.2. Изготовление ключей Центра Регистрации

1. Администратор ЦР устанавливает сертификат ЦС на ПЭВМ ЦР. Рекомендуется обеспечить защищенную доставку и хранение сертификата ЦС на ПЭВМ.
2. Администратор ЦР производит формирование личного закрытого ключа ЦР и запроса на сертификат, содержащего открытый ключ ЦР. С закрытого ключа ЦР формируется резервная копия, которая хранится у начальника УЦ. Пометка о формировании ключа и запроса на сертификат заносится в «Журнале пользователя сети».
3. Бланк запроса на сертификат выводится на принтер в двух экземплярах и заверяется администратором ЦР.
4. Запрос на сертификат записывается на магнитный носитель (дискету).
5. Администратор ЦР прибывает в УЦ, где администратор ЦС производит формирование сертификата ЦС, используя для этого полученный запрос на сертификат и бумажный бланк запроса. Бланк запроса на сертификат заверяется администратором ЦС. Одна копия бланка запроса хранится у администратора ЦС, другая - у администратора ЦР.
6. Администратор ЦС выводит на принтер бланк сертификата ЦР в двух экземплярах. Бланк сертификата ЦР сверяется с бланком запроса и заверяется администраторами ЦС, ЦР и начальником УЦ.
7. Администратор ЦР получает личный сертификат ЦР на магнитном носителе и заверенный бланк сертификата ЦР.
8. Администратор ЦР, используя ПО ЦР, устанавливает сертификат на ПЭВМ ЦР.

После завершения этих действий Центр Сертификации и Центр Регистрации готовы к регистрации пользователей системы и выпуску сертификатов.

7.5. Формирование ключей пользователя

7.5.1. Регистрация пользователя

1. Руководство организации-пользователя для регистрации пользователя в сети должно представить в УЦ на имя его начальника с сопроводительным письмом следующие документы (конкретный состав документов определяется Регламентом (Договором) системы:

1) лист с образцами печати и личной подписи руководителя организации;

2) копию Договора (Временного соглашения) с администрацией системы;

3) выписку из приказа о назначении администратора информационной безопасности организации (заместителя), заверенную подписью руководства и печатью организации;

4) заполненные и заверенные листки по учету кадров на администратора безопасности организации (заместителя).

2. Администратор Центра Регистрации на основании полноты и достаточности предоставленных документов производит регистрацию пользователя в системе.

3. Данные регистрации пользователя выводится на принтер в двух экземплярах и заверяется администратором ЦР и пользователем. Один экземпляр бланка регистрации хранится у администратора ЦР, второй экземпляр – у пользователя.

4. Администратор ЦР выдает пользователю карточку оповещения о компрометации, в которой отражаются телефоны и пароли УЦ и пользователя, Рисунок 8.1.

Карточка оповещения используется участниками системы для сообщений о компрометации ключа по телефонным каналам общего пользования, для этого в ней указаны телефоны УЦ, пароль (кодовое слово) администратора УЦ и уникальный пароль (кодовое слово), присвоенный пользователю УЦ. Карточка оповещения должна храниться у пользователя наравне с ключами.

Пароль УЦ	Основной пароль	Резервный пароль
Телефоны Администратора ЦР (УЦ)		
Пароль пользователя	Основной пароль	Резервный пароль

Рисунок 8.1 - Карточка оповещения о компрометации.

5. При наличии системы электронной почты и зарегистрированного почтового адреса пользователя, администратор ЦР добавляет его в список рассылки пользователей системы, который используется для централизованного оповещения пользователей системы.

6. Администратор ЦР делает запись в «Журнале регистрации администраторов безопасности и пользователей».

7. При завершении регистрации каждого пользователя системы администратор ЦС (ЦР) передает пользователю копию бланка сертификата ЦС, сертификат и СОС ЦС (ЦР).

7.5.2. Формирование личных ключей пользователя

При наличии в организации администратора безопасности, все описанные ниже действия могут производиться либо администратором безопасности, либо пользователем в присутствии администратора безопасности.

1. Пользователь устанавливает сертификат и СОС ЦС (ЦР) в справочник сертификатов. Требуется обеспечить защищенную доставку и хранение сертификата ЦС на ПЭВМ пользователя.

2. Пользователь производит формирование личного ключа ЭП и запроса на сертификат, содержащего ключ проверки ЭП пользователя.

3. Бланк запроса на сертификат выводится на принтер в двух экземплярах и заверяется пользователем, (администратором безопасности при его наличии) и ответственными лицами (например, директором и главным бухгалтером).

4. При отсутствии сетевого взаимодействия организации с ЦР, запрос записывается на магнитный носитель (дискету) для передачи в ЦР.

5. При наличии сетевого взаимодействия организации с ЦР, запрос на сертификат может быть передан по сети. При этом необходимо обеспечить подтверждение владения закрытым ключом пользователем. Для этого запрос на сертификат может быть послан в виде сообщения, подписанного предыдущим ключом пользователя.

6. Если запрос был записан на магнитный носитель, пользователь (администратор безопасности) прибывают в Центр Сертификации (УЦ) вместе с записанным запросом и заверенными бланками запроса.

7. Если запрос на сертификат был передан по сети, пользователь (администратор безопасности) должны передать обе копии бланка запроса в Центр Сертификации, используя для этого доступные способы доставки (например, заказное письмо).

8. При получении запроса на сертификат администратор ЦС производит формирование сертификата пользователя. Сертификат пользователя хранится в базе ЦС в течение установленного срока хранения (равного сроку действия сертификата).

9. Администратор ЦС выводит на принтер две копии бланка сертификата пользователя и делает запись о формировании сертификата в «Журнале пользователя сети».

7.5.3. Получение личного сертификата пользователем

Личный сертификат может быть получен следующими способами:

– при личном присутствии пользователя (администратора безопасности) в УЦ;

– по сети с использованием зарегистрированного адреса электронной почты или в процессе непосредственного соединения с центром.

В любом из перечисленных случаев сертификат не передается пользователю до тех пор, пока Центр Регистрации не получит заверенный бланк запроса на сертификат.

При передаче личного сертификата пользователю ему также передается заверенный администратором бланк запроса и сертификата пользователя. Вторые копии этих бланков хранятся в ЦС (ЦР).

7.6. Повторная регистрация пользователя

Повторная регистрация пользователя в Центре Регистрации производится в случае изменения зарегистрированных атрибутов пользователя по инициативе пользователя либо администрации системы.

7.7. Плановая смена ключей

7.7.1. Смена ключей Центра Сертификации

Заблаговременно (до окончания срока действия закрытого ключа ЦС) администратор ЦС производит формирование нового закрытого ключа и сертификата ЦС (см. 7.2 «Формирование ключей Центра Сертификации»).

Сформированный новый сертификат ЦС записывается на магнитный носитель (дискету) и передается в ЦР вместе с бланком сертификата.

При окончании действия закрытого ключа, ключевые носители с закрытым ключом, а также копии закрытого ключа ЦС уничтожаются по Акту комиссией.

Все пользователи системы до окончания срока действия закрытого ключа ЦС обязаны получить новый сертификат ЦС и добавить его в справочники сертификатов, без удаления действующего сертификата ЦС.

7.7.2. Смена ключей Центра Регистрации

Заблаговременно (до окончания срока действия закрытого ключа ЦС) администратор ЦР производит формирование нового закрытого ключа и сертификата ЦР.

Смена ключей Центра Регистрации производится аналогично смене ключей пользователя (см. 7.7.3 «Смена ключей пользователя»).

Все пользователи системы до окончания срока действия закрытого ключа ЦР обязаны получить новый сертификат ЦР.

7.7.3. Смена ключей пользователя

Пользователь, имеющий действующий сертификат и соответствующий ему ключ ЭП, в любой момент времени (но не позднее недели) до окончания срока действия действующего закрытого ключа, может произвести формирование нового ключа ЭП.

Формирование нового ключа ЭП, запроса на сертификат, передача запроса в ЦР и получение сертификата производится согласно последовательности, описанной в разделе 7.5 «Формирование ключей пользователя».

Ключевые носители с ключом ЭП, срок действия которого истек, уничтожаются путем переформатирования (очистки), о чем делается запись в «Журнале пользователя сети».

7.8. Компрометация ключей

Определение термина компрометация, виды компрометации и основные события, приводящие к компрометации, приведены в разделе «Основные термины и понятия».

По факту компрометации ключей и/или носителей должно быть проведено служебное расследование.

Информация с выведенных из действия скомпрометированных ключевых носителей после проведения служебного расследования уничтожается, о чем делается запись в «Журнале пользователя сети».

7.8.1. Компрометация ключей Центра Сертификации

В случае компрометации ключа Центра Сертификации вся система должна быть остановлена.

При наличии резервных ключей, система должна полностью перейти на комплект резервных ключей.

Если резервные ключи не были предусмотрены, для восстановления системы необходимо:

1. Повторно произвести формирование ключа и сертификата ЦС;
2. Сформировать СОС ЦС, с указанием в нем отзываемого сертификата ЦС;
3. Обеспечить получение сертификата и СОС ЦС всеми пользователями системы;
4. Произвести выпуск новых сертификатов всех пользователей, используя действующие сертификаты;
5. Обеспечить получение новых личных сертификатов пользователями системы.

7.8.2. Компрометация ключей Центра Регистрации

Компрометация ключа ЦР не приводит к останову системы. В случае компрометации становится невозможным сетевое взаимодействие между пользователем системы и ЦР в части управления ключевой системой.

В случае компрометации ключа Центра Регистрации должны быть выполнены следующие мероприятия:

1. ЦС формирует СОС, с указанием в нем отзываемого сертификата ЦР;
2. При наличии резервных ключей ЦР, ЦР переходит на резервный ключ.

Если резервные ключи не были предусмотрены, то для восстановления системы необходимо:

1. Повторно произвести формирование ключа и сертификата ЦР;
2. Обеспечить получение сертификата ЦР всеми пользователями системы (в случае сетевого взаимодействия).

7.8.3. Компрометация ключей пользователя

При компрометации ключа у пользователя он должен немедленно прекратить связь по сети с другими пользователями.

Пользователь (или администратор безопасности организации) должен немедленно известить ЦР (УЦ) о компрометации ключей пользователя.

Информация о компрометации может передаваться в УЦ по телефону с сообщением заранее условленного пароля, зарегистрированного в «Карточке оповещения о компрометации».

После компрометации ключей пользователь формирует новый закрытый ключ и запрос на сертификат. Так как пользователь не может использовать скомпрометированный ключ для формирования ЭП и передачи запроса в защищенном виде по сети, запрос на сертификат вместе с бланками доставляется лично пользователем (администратором безопасности) в Центр Регистрации.

7.8.4. Действия УЦ при компрометации ключей пользователя

При получении сообщения о компрометации ключа одного из пользователей сети, администратор ЦР оповещает ЦС о необходимости добавления сертификата, соответствующего скомпрометированному закрытому ключу/ключу ЭП в список отозванных сертификатов. ЦС, при формировании очередного СОС, включает в него отзываемый сертификат.

Дата, с которой сертификат считается недействительным в системе, устанавливается равной дате изготовления СОС, в который был включен отзываемый сертификат.

При наличии сетевых средств распространения СОС, администратор ЦР производит публикацию СОС.

Для рассылки вновь изданного СОС всем пользователям, зарегистрированным в списке рассылки (см. 7.5.1 «Регистрация пользователя»), может быть использована электронная почта.

Сертификат открытого ключа/ключа проверки ЭП пользователя не удаляется из базы ЦС (ЦР) и хранится в течение установленного срока хранения для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением ЭП.

7.9. Исключение пользователя из сети

Исключение пользователя из сети может быть осуществлено на основании письменного заявления пользователя в адрес начальника УЦ, заверенного руководством организации. Исключение пользователя из сети производится аналогично действиям при компрометации ключа пользователя. Получив такое заявление, администратор ЦР производит действия, описанные в разделе 7.8.4 «Действия УЦ при компрометации ключей пользователя».

7.10. Периодичность издания СОС

Периодичность издания СОС Центром Сертификации определяется администрацией системы.

Центр Сертификации может ежедневно издавать СОС и публиковать его в сетевом справочнике (при его наличии).

Для распространения вновь изданного СОС может быть использована система электронной почты и список рассылки пользователей системы, который формируется при регистрации пользователя (см. 7.5.1 «Регистрация пользователя»).

Пользователи должны регулярно обновлять СОС, хранящийся в локальном справочнике сертификатов с использованием доступных средств.

7.11. Ведение журналов

Администратор УЦ ведет следующие журналы:

– «Журнал регистрации администраторов безопасности и пользователей»;

– «Журнал пользователя сети».

Администраторы безопасности организации ведут журнал «Журнал пользователя сети».

В «Журнале регистрации администраторов безопасности и пользователей» фиксируются факты регистрации администраторов ЦС (ЦР), администраторов безопасности организации, пользователей системы.

В «Журнал пользователя сети» записываются факты изготовления и плановой смены ключей, факты компрометации ключевых документов, нештатные ситуации, происходящие в сети, проведение регламентных работ, данные о полученных у администратора безопасности организации ключевых носителях, нештатных ситуациях, произошедших на АРМ с установленным ПО СКЗИ.

В «Журнале пользователя сети» может отражаться следующая информация:

– дата, время;

– запись о компрометации ключа;

– запись об изготовлении личного ключевого носителя пользователя, идентификатор носителя;

– запись об изготовлении копий личного ключевого носителя пользователя, идентификатор носителя;

– запись об изготовлении резервного ключевого носителя пользователя, идентификатор носителя

– запись о получении сертификата открытого ключа или ключа проверки ЭП, полный номер ключевого носителя, соответствующий сертификату;

– записи, отражающие выдачу на руки пользователям (ответственным исполнителям) и сдачу ими на хранение личных ключевых носителей, включая резервные ключевые носители;

– события, происходившие на АРМ пользователя с установленным ПО СКЗИ, с указанием причин и предпринятых действий;

Ориентировочные графы журналов приведены в приложениях (см. Приложение В).

8. Разбор конфликтных ситуаций, связанных с применением ЭП

Применение электронной подписи в автоматизированной системе может приводить к конфликтным ситуациям, заключающимся в оспаривании сторонами (участниками системы) авторства и/или содержимого документа, подписанного электронной подписью.

Разбор подобных конфликтных ситуаций требует применения специального программного обеспечения для выполнения проверок и документирования данных, используемых при выполнении процедуры проверки соответствия ЭП содержимому электронного документа.

Разбор конфликтной ситуации заключается в доказательстве авторства подписи конкретного электронного документа конкретным исполнителем.

Данный разбор основывается на математических свойствах алгоритмов ЭП, реализованных в соответствии со стандартами РФ ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и ГОСТ Р 34.11-94, гарантирующих невозможность подделки значения ЭП любым лицом, не обладающим закрытым ключом подписи.

При проверке значения ЭП используется ключ проверки ЭП, значение которого вычисляется по значению ключа ЭП при их формировании.

В системе должны быть предусмотрены средства ведения архивов электронных документов с ЭП и сертификатов ключей проверки ЭП.

Разбор конфликтной ситуации выполняется комиссией, состоящей из представителей сторон, службы безопасности и экспертов. Состав комиссии, порядок ее формирования, регламент работы, рассмотрение результатов определяется в приложении к Регламенту (Договору), заключаемому между участниками информационного обмена.

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

8.1. Порядок разбора конфликтной ситуации

Разбор конфликтной ситуации выполняется по инициативе любого участника информационного обмена и состоит из:

1. предъявления претензии одной стороны другой;
2. формирования комиссии;
3. разбора конфликтной ситуации;
4. взыскания с виновной стороны принесенного ущерба.

Разбор конфликтной ситуации проводится с использованием программного обеспечения СКЗИ «КриптоПро CSP» v 4.0 R4 для электронного документа, авторство или содержание которого оспаривается.

Проверка подписанного электронного документа включает в себя выполнение следующих действий:

1. определение сертификата или нескольких сертификатов, необходимых для проверки ЭП;
2. проверка ЭП электронного документа с использованием каждого сертификата;
3. определение даты формирования каждой ЭП в электронном документе;
4. проверка ЭП каждого сертификата, путем построения цепочки сертификатов до сертификата Главного ЦС;
5. проверка действительности сертификатов на текущий момент времени;
6. проверка действительности сертификатов на момент формирования ЭП;
7. проверка отсутствия сертификатов в СОС.

При проверке ЭП документа, верификации цепочки сертификатов, отсутствии сертификата в СОС, авторство подписи под документом считается установленным.

	Несовпадение даты формирования документа и сроков действия сертификата и/или сроков действия ключа ЭП '& на определение авторства документа. В таком случае можно сделать предположение о несоблюдении пользователем Регламента (Договора) в части сроков действия ключей, сертификатов или некорректного использования сертификата в прикладном ПО.

8.2. Случаи невозможности проверки значения ЭП

При не обнаружении в архиве сертификата открытого ключа (ключа проверки ЭП) пользователя, выполнившего ЭП, доказать авторство документа невозможно. В связи с этим, архив с сертификатами открытых ключей необходимо подвергать регулярному резервному копированию и хранить в течение всего установленного срока хранения.

9. Нештатные ситуации при эксплуатации СКЗИ

В Таблице 11.1 приведен основной перечень нештатных ситуаций и соответствующие действия персонала при их возникновении.

Таблица 11.1 - Действия персонала в нештатных ситуациях

№ п/п	Нештатная ситуация	Действия персонала
1.	Эвакуация, угроза нападения, взрыва и т.п., стихийные бедствия, аварии общего характера в Центре управления ключевой системой.	Остановить все ЭВМ. Персонал, имеющий доступ к ключам, обязан сдать все имеющиеся у него в наличии ключевые носители администратору безопасности. Администратор безопасности упаковывает все ключевые носители, регистрационные карточки сертификатов открытых ключей пользователей, сертификаты ключей проверки ЭП пользователей в опечатываемый контейнер, который выносит в безопасное помещение или здание. Опечатанный контейнер должен находиться под охраной до окончания действия нештатной ситуации и восстановления нормальной работы аппаратных и программных средств СКЗИ. Администратор безопасности оповещает по телефонным каналам общего пользования всех пользователей о приостановке работы системы. В случае наступления события, повлекшего за собой долговременный выход из строя аппаратных средств СКЗИ, администратор безопасности уничтожает всю ключевую информацию с носителей, находящихся в контейнере.
2.	Компрометация одного из личных ключевых носителей.	Порядок действий при компрометации ключей описан в разделе 7.8.3 «Компрометация ключей пользователя».
3.	Выход из строя первого личного ключевого носителя.	Необходимо сообщить по телефону в УЦ о факте выхода из строя личного ключевого носителя и обеспечить его доставку в УЦ для выяснения причин выхода из строя. Для работы используется второй личный ключевой носитель.
4.	Выход из строя второго личного ключевого носителя (при условии, что первый тоже вышел из строя).	Пользователь, у которого вышли из строя оба личных ключевых носителя, является в УЦ для повторной регистрации (без изменения данных регистрации).
5.	Отказы и сбои в работе аппаратной части АРМ со встроенным СКЗИ.	При отказах и сбоях в работе аппаратной части АРМ со встроенным СКЗИ необходимо остановить работу, по возможности локализовать неисправность и в дальнейшем произвести ремонт в установленном порядке и, при необходимости, переустановку СКЗИ.
6.	Отказы и сбои в работе средств защиты от НСД.	При отказах и сбоях в работе средств защиты от НСД, администратор безопасности, должен восстановить работоспособность средств НСД. При необходимости переустановить программно-аппаратные средства НСД.
7.	Утеря личного ключевого носителя.	Утеря личного ключевого носителя приводит к компрометации хранящегося в нем ключа. Порядок действий при компрометации ключей описан в разделе 7.8.3 «Компрометация ключей пользователя».
8.	Отказы и сбои в работе программных средств вследствие не выявленных ранее ошибок в программном обеспечении.	При отказах и сбоях в работе программных средств, вследствие не выявленных ранее ошибок в программном обеспечении, необходимо остановить работу, локализовать по возможности причину отказов и сбоев и вызвать разработчика данного ПО или его представителя для устранения причин, вызывающих отказы и сбои.

№ п/п	Нештатная ситуация	Действия персонала
9.	Отказы в работе программных средств вследствие случайного или умышленного их повреждения.	При отказах в работе программных средств, вследствие случайного или умышленного их повреждения, лицо, ответственное за безопасность функционирования программных и аппаратных средств, обязано произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы программных средств в установленном порядке.
10.	Отказы в работе программных средств вследствие ошибок оператора.	При отказах в работе программных средств, вследствие ошибок оператора, оператор сообщает о данном факте лицу, ответственному за безопасность функционирования программных и аппаратных средств. Ответственный за безопасность функционирования программных и аппаратных средств дает соответствующие указания обслуживающему персоналу по восстановлению правильной работы программных средств в установленном порядке.

Все нештатные ситуации должны отражаться в «Журнале пользователя сети» (см. п.7.11).

10. Применение «КриптоПро CSP» v. 4.0 R4

Возможны следующие применения «КриптоПро CSP» v. 4.0 R4

1. Применение «КриптоПро CSP» v. 4.0 R4 в составе стандартного программного обеспечения Microsoft и других компаний, использующих криптографический интерфейс в соответствии с архитектурой Microsoft.

2. Встраивание «КриптоПро CSP» v. 4.0 R4 во вновь разрабатываемое или существующее прикладное программное обеспечение.

11. Использование СКЗИ в стандартном программном обеспечении

Программное обеспечение СКЗИ позволяет использовать российские криптографические алгоритмы и сертификаты открытых ключей стандарта X.509 совместно со следующим программным обеспечением Microsoft:

– Центр Сертификации - Microsoft Certification Authority, входящий в состав Windows 2000 Server, Advanced Server, Windows 2003 Server, Windows 2008 Server, Windows 2008R2 Windows 2012.

– Электронная почта - MS Outlook (Office 2003, Office 2007, Office 2010, Office 2013, Office 2016).

– Электронная почта - Microsoft Outlook Express в составе Internet Explorer/Microsoft Edge, Почта Windows Mail, Live Mail.

– Microsoft Word, Excel из состава Microsoft Office 2003, 2007, 2010, 2013, 2016 (с помощью плагина КриптоПро Office Signature).

– Microsoft Exchange Server 2010, 2013.

– Средства контроля целостности ПО, распространяемого по сети - Microsoft Authenticode.

– Службы терминалов для Windows 2003 Server, Windows 2008 Server, Windows 2008R2 Server, Windows 2012 Server (включая шлюз служб терминалов).

– Защита TCP/IP соединений в сети Интернет - протокол TLS/SSL при взаимодействии Internet Explorer/Microsoft Edge – web-сервер IIS, TLS-сервер, TLS-клиент (IE).

– Приложение командной строки для формирования запроса на сертификат certreq.

– SQL-сервер.

– ISA сервер.

– Сервер TMG.

– Сервер UAG.

– Сервер терминалов и клиент (RDP).

Под управлением UNIX-подобных ОС СКЗИ используется совместно со следующим программным обеспечением:

– Apache Trusted TLS (Digt).

– Trusted TLS (Digt).

Используется совместно с Adobe Reader или Adobe Acrobat для создания/проверки усовершенствованной ЭП pdf файлов (см. ЖТЯИ.00064-01 90 02. КриптоПро PDF. Руководство по автоматизации создания и проверки электронных подписей).

Примечание: Использование СКЗИ в стандартном программном обеспечении должно осуществляться в соответствии с п. 2 Правил пользования ЖТЯИ.00087-03 95 01.

Российские криптографические алгоритмы и сертификаты открытых ключей X.509 используются с указанным программным обеспечением в соответствии со следующими международными и российскими рекомендациями:

– 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 (rfc4491) описывает использование российских криптографических алгоритмов в инфраструктуре открытых ключей интернет (PKIX, Internet X.509 Public Key Infrastructure). В данном документе описаны форматы представления открытых ключей ЭП, используемых для создания сертификатов открытых ключей и списков отозванных сертификатов X.509, идентификаторы алгоритмов, соответствие параметров криптографических алгоритмов их идентификаторам.

– 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 (rfc4357) описывает дополнительные алгоритмы,

необходимые для использования ГОСТ 28147-89, ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94. В их число входят: режимы дополнения данных для блочного шифрования по ГОСТ 28147-89 и CBC, блочное шифрование с зацеплением (режим шифрования CBC), ключевое хэширование (HMAC на базе ГОСТ Р 34.11-94), преобразование ключа и синхропосылки после обработки очередных 1 Кб данных, генерация псевдослучайной последовательности (аналог PRF на базе HMAC), формирование ключа обмена (согласования) на базе ГОСТ Р 34.10-2001, формирование ключа экспорта рабочего ключа, диверсификация ключа, экспорт рабочего ключа на ключе экспорта, экспорт рабочего ключа на ключе обмена, наборы стандартных параметров алгоритмов (например, для шифрования - узел замены, режим шифрования, алгоритм усложнения ключа), задаваемые идентификаторами.

– Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94 and GOST R 34.10-2001 algorithms with the Cryptographic Message Syntax (CMS) (rfc4490) описывает использование российских криптографических алгоритмов в документах, удовлетворяющих стандарту CMS (Cryptographic Message Syntax), в частности, применяемом для обмена защищёнными сообщениями по электронной почте и являющимся стандартом на представление электронного документа в защищенном виде с использованием электронной подписи и шифрования. Для шифрованных сообщений описаны оба варианта: обмен ключами и транспорт ключа (key agreement и key transport).

– «Addition of GOST Ciphersuites to Transport Layer Security (TLS)» (draft-chudov-cryptopro-cptls-01) является дополнением к спецификации RFC 2246 в части описания применения российских алгоритмов. Протокол TLS(SSL) широко используется для защиты сетевых соединений, и, в частности, для защищенного доступа к Веб-сайтам (HTTPS). Документ описывает четыре механизма (Cipher Suites), реализующих ключевые протоколы при использовании открытых ключей ГОСТ Р 34.10-2001. Первые два используют шифрование ГОСТ 28147-89 и контроль целостности с помощью имитовставки, третий и четвертый не используют шифрование и контролируют целостность с помощью значения ключевой хэш–функции (MAC) на основе алгоритма ГОСТ Р 34.11-94.

– «Using algorithms GOST R 34.10-2001, GOST R 34.10-94 and GOST R 34.11-94 for XML Digital Signatures» (draft-chudov-cryptopro-cpxmldsig-00) является дополнением к существующему документу, описывающему правила применения ЭП в документах формата XML «XML-Signature Syntax and Processing», принятому консорциумом W3C, в части использования российских алгоритмов электронно-цифровой подписи.

– Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Системы обработки информации. Защита криптографическая. Методические рекомендации по криптографическим алгоритмам, сопутствующим применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012».

– Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Техническая спецификация. Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509».

– Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)».

– Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS».

– Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Системы обработки информации. Защита криптографическая. Рекомендации по стандартизации. Задание параметров эллиптических кривых в соответствии с ГОСТ Р 34.10-2012».

– Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Системы обработки информации. Защита криптографическая. Методические рекомендации по заданию узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89».

– Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Системы обработки информации. Защита криптографическая. Техническая спецификация по использованию ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при согласовании ключей в протоколах IKE ISAKMP».

– Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Системы обработки информации. Защита криптографическая. Техническая спецификация по использованию дополнительных узлов замены ГОСТ 28147-89 для шифрования вложений IPsec ESP»

– Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Системы обработки информации. Защита криптографическая. Техническая спецификация по использованию ГОСТ Р 34.11-94 при обеспечении целостности в протоколах IPsec AH и ESP.

12. Использование СКЗИ с программными продуктами разработки ООО «КРИПТО-ПРО»

СКЗИ может использоваться совместно со следующими программными продуктами разработки ООО «КРИПТО-ПРО» при наличии сертификата соответствия ФСБ России:

- «КриптоПро УЦ»;
- «КриптоПро OCSP»;
- «КриптоПро TSP»;
- «КриптоАРМ»;
- «КриптоПро SSF»;
- «Клиент КриптоПро HSM»;
- «КриптоПро PDF».

13. Встраивание СКЗИ

Архитектура СКЗИ обеспечивает возможность его встраивания в различные программно-аппаратные среды.

СКЗИ может быть использовано прикладным программным обеспечением с помощью загрузки модуля вызовом функции LoadLibrary(). Для этих целей в комплект поставки включается документ ЖТЯИ.00087-03 96 01. «Руководство программиста», описывающий состав функций и тестовое ПО. При такой реализации прикладному ПО доступен лишь ограниченный набор низкоуровневых криптографических функций, соответствующий интерфейсу Microsoft CSP.

При использовании СКЗИ под управлением операционной системы iOS загрузка библиотек при помощи функции LoadLibrary() невозможна. Для этой операционной системы встраивание должно производиться в соответствии с документацией, входящей в состав фреймворка для разработки. Программный интерфейс, предоставляемый СКЗИ под управлением iOS, также описан в документе «ЖТЯИ.00087-03 96 01. «КриптоПро CSP. «Руководство программиста» и соответствует интерфейсу Microsoft CSP.

14. Требования по защите от НСД

14.1. Общие требования по организации работ по защите от НСД

Защита аппаратного и программного обеспечения от НСД при установке и использовании СКЗИ «КриптоПро CSP» v 4.0 R4 является составной частью общей задачи обеспечения безопасности информации в системе, в состав которой входит СКЗИ.

Наряду с применением средств защиты от НСД необходимо выполнение приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации, а также установление соответствующих правил для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

Защита информации от НСД должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль должен периодически выполняться администратором безопасности на основе требований документации на средства защиты от НСД.

В организации, эксплуатирующей СКЗИ, должен быть назначен администратор безопасности, на которого возлагаются задачи организации работ по использованию СКЗИ, выработки соответствующих инструкций для пользователей, а также контроль за соблюдением требований по безопасности.

è $ $
$ $

Правом доступа к рабочим местам с установленными СКЗИ должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, применяющего СКЗИ, с документацией на СКЗИ, а также с другими нормативными документами, созданными на её основе.

14.2. Требования по размещению технических средств с установленным СКЗИ.

Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным СКЗИ, посторонних лиц, не допущенных к работе на данных технических средствах. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями для пресечения негативных воздействий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию.

Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ, сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

Размещение СКЗИ «КриптоПро CSP» v 4.0 R4 в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.

14.3. Требования по установке СКЗИ, общесистемного и специального ПО на ПЭВМ

ПЭВМ, на которых используется СКЗИ, должны быть допущены для обработки конфиденциальной информации по действующим в Российской Федерации требованиям по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К), с учетом модели угроз в информационной системе заказчика, которым должно противостоять СКЗИ «КриптоПро CSP» v 4.0 R4.

Инсталляция СКЗИ «КриптоПро CSP» v 4.0 R4 на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.

К установке общесистемного и специального программного обеспечения, а также СКЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и на СКЗИ.

При установке программного обеспечения СКЗИ следует:

– На технических средствах, предназначенных для работы с СКЗИ, использовать только лицензионное программное обеспечение фирм–изготовителей.

– При установке ПО СКЗИ на ПЭВМ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ и совместно поставляемых с СКЗИ компонент СФК.

– На ПЭВМ не должны устанавливаться средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти СКЗИ и приложений, использующих СКЗИ, а также для просмотра кода и памяти СКЗИ и приложений, использующих СКЗИ, в процессе обработки СКЗИ защищаемой информации и/или при загруженной ключевой информации.

– Предусмотреть меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлены СКЗИ (например, путем опечатывания системного блока и разъемов ПЭВМ).

– После завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО СКЗИ, а также его окружения в соответствии с документацией.

– Программное обеспечение, устанавливаемое на ПЭВМ с СКЗИ не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

14.4. Меры по обеспечению защиты от НСД

При использовании СКЗИ должны выполняться следующие меры по защите информации от НСД:

– Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому;

▪ периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев.

– Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС;

– Средствами BIOS должна быть исключена возможность работы на ПЭВМ с СКЗИ, если во время её начальной загрузки не проходят встроенные тесты;

– В качестве меры по усилению защиты от НСД следует запретить сохранение паролей, используемых в работе СКЗИ. Для этого предпочтительнее воспользоваться групповыми политиками, включить групповую политику «Запретить использование сохраненных паролей»:

Конфигурация компьютера\Административные шаблоны\Классические административные шаблоны\КРИПТО-ПРО\Крипто-про CSP

Или в ветку системного реестра

HKLM\SOFTWARE[\Wow6432Node]\CryptoPro\Cryptography\CurrentVersion\Parameters

добавить значение

DisableSavedPasswords (DWORD) = 1.

При эксплуатации СКЗИ ЗАПРЕЩАЕТСЯ:

– оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации;

– вносить какие-либо изменения в программное обеспечение СКЗИ;

– осуществлять несанкционированное администратором безопасности копирование ключевых носителей;

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации (за исключением случаев, предусмотренных данными правилами);

– использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;

– записывать на ключевые носители постороннюю информацию;

– использовать несъемные ключевые носители;

– вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя;

– подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией;

– работать на компьютере, если во время его начальной загрузки не проходит встроенный тест ОЗУ, предусмотренный в ПЭВМ;

– вносить какие-либо изменения в программное обеспечение СКЗИ;

– изменять настройки, установленные программой установки СКЗИ или администратором;

– использовать синхропосылки, вырабатываемые не средствами СКЗИ;

– обрабатывать на ПЭВМ, оснащенной СКЗИ, информацию, содержащую государственную тайну;

– использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ «КриптоПро CSP» v 4.0 R4;

– осуществлять несанкционированное вскрытие системных блоков ПЭВМ;

– приносить и использовать в помещении, где размещены средства СКЗИ, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер);

Администратор безопасности должен сконфигурировать операционную систему, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

– недопустимо использовать нестандартные, измененные или отладочные версии ОС;

– необходимо исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;

– необходимо исключить возможность удаленного управления, администрирования и модификации ОС и её настроек;

– на ПЭВМ должна быть установлена только одна операционная система;

– правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности;

– все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);

– режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;

– всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права;

– необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

- системный реестр;
- файлы и каталоги;
- временные файлы;
- журналы системы;
- файлы подкачки;
- кэшируемая информация (пароли и т.п.);
- отладочная информация.

Кроме вышеперечисленного, необходимо организовать стирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям (п.6.7 ЖТЯИ.00087–01 91 01. Руководство администратора безопасности общая часть).

– должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;

– необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;

– в случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети;

– при использовании СКЗИ на ПЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей должны использоваться дополнительные методы и средства защиты (например, установка межсетевых экранов, организация VPN сетей и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации;

– организовать и использовать систему аудита, организовать регулярный анализ результатов аудита;

– организовать и использовать комплекс мероприятий антивирусной защиты;

– должно быть запрещено использование СКЗИ для защиты речевой информации;

– должна быть запрещена работа СКЗИ при включенных в ПЭВМ штатных средствах выхода в радиоканал.

Рекомендуется аппаратуру, на которой устанавливается СКЗИ, проверить на отсутствие аппаратных закладок.

14.5. Требования по подключению СКЗИ для работы по общедоступным каналам передачи данных

1. Порядок подключения СКЗИ к каналам связи должен быть определен эксплуатирующей организацией. Лицом, ответственным за безопасность работы СКЗИ по общедоступным каналам, как правило, должен быть администратор безопасности.

2. При подключении СКЗИ к общедоступным каналам передачи данных должна быть обеспечена безопасность защищенной связи. При этом должны быть определены:

– Порядок подключения СКЗИ к каналам.

– Выделено лицо, ответственное за безопасность работы по общедоступным каналам.

– Разработан типовой регламент защищенной связи, включающий:

  ▪ политику безопасности защищенной связи.

  ▪ допустимый состав прикладных программных средств, для которого должно быть исследовано и обосновано отсутствие негативного влияния на СКЗИ по каналу передачи данных.

  ▪ перечень допустимых сетевых протоколов.

  ▪ защиту сетевых соединений (перечень допустимых сетевых экранов).

  ▪ систему и средства антивирусной защиты.

3. Перечень стандартных средств ОС, может включаться администратором в типовой регламент без проведения дополнительных исследований по оценке их влияния на СКЗИ. При этом должны выполняться следующие условия:

– своевременное обновление программных средств, включенных в состав регламента;

– контроль среды функционирования СКЗИ;

– определение и контроль за использованием сетевых протоколов;

– соблюдение правил пользования СКЗИ и среды функционирования СКЗИ.

4. Должен быть обеспечен организационно-технический контроль запросов на установление соединения абонентов по протоколу TLS с использованием эфемерных ключей, исключающий возможность использования абонентом не своих атрибутов соединения (такие, как Client_Id и т.п.).

5. При использовании СКЗИ с другими стандартными программными средствами, возможность подключения СКЗИ к общедоступным каналам передачи данных должна быть определена только после проведения дополнительных исследований с оценкой невозможности негативного влияния нарушителя на функционирование СКЗИ, использующего возможности общедоступных каналов.

14.6. Требования по использованию в СКЗИ программно-аппаратных средств защиты от НСД

В качестве программно-аппаратных средств защиты от НСД в СКЗИ могут использоваться Программно-аппаратный комплекс «КРИПТОН-ЗАМОК», электронный замок «Соболь», АМДЗ «Аккорд» и АПМДЗ «МАКСИМ-М1». Идентификационные данные указанных средств приведены в документе «ЖТЯИ.00087-03 30 01. КриптоПро CSP. Формуляр», п.3.10.

14.6.1. Электронный замок «Соболь»

Система Электронный замок предназначена для организации защиты компьютера от входа посторонних пользователей. Под посторонними пользователями понимаются все лица, не зарегистрированные в системе Электронный замок как пользователи данного компьютера.

Электронный замок «Соболь» используется на платформах

- Windows;
- Linux;
- FreeBSD.

Электронный замок «Соболь» обеспечивает:

- регистрацию пользователей компьютера и назначение им персональных идентификаторов и паролей на вход в систему;
- запрос персонального идентификатора и пароля пользователя при загрузке компьютера;
- возможность блокирования входа в систему зарегистрированного пользователя;
- ведение системного журнала, в котором производится регистрация событий, имеющих отношение к безопасности системы;
- контроль целостности файлов на жестком диске (только в ОС Windows);
- контроль целостности физических секторов жесткого диска (только в ОС Windows);
- аппаратную защиту от несанкционированной загрузки операционной системы с гибкого диска и CD-ROM диска.

Установка и настройка электронного замка на АРМ пользователя должна производиться в соответствии с эксплуатационной документацией. Перед эксплуатацией электронного замка в составе АРМ пользователя необходимо ознакомиться с комплектом документации (в соответствии с паспортом УВАЛ.00300-58 ПС) на данный комплекс и принять рекомендуемые в документации защитные организационные меры.

Настройка электронного замка на требуемую конфигурацию выполняется администратором безопасности. Настройка должна исключать возможность вмешательства пользователя в процессы загрузки операционной системы и прикладного ПО и проверки целостности программной среды.

15. Требования по криптографической защите

Должны выполняться следующие требования по криптографической защите:

1. Использование только лицензионного системного программного обеспечения.

2. Настройки операционных систем для работы с СКЗИ, включенные в следующие документы:

ЖТЯИ.00087-03 91 02 Руководство администратора безопасности. Windows,

ЖТЯИ.00087-03 91 03 Руководство администратора безопасности. Linux,

ЖТЯИ.00087-03 91 04 Руководство администратора безопасности. FreeBSD,

ЖТЯИ.00087-03 91 05 Руководство администратора безопасности. Solaris,

ЖТЯИ.00087-03 91 06 Руководство администратора безопасности. AIX,

ЖТЯИ.00087-03 91 07 Руководство администратора безопасности. Mac OS,

ЖТЯИ.00087-03 91 08 Руководство администратора безопасности. iOS.

ЖТЯИ.00087-03 91 09 Руководство администратора безопасности. Виртуальные среды.

ЖТЯИ.00087-03 91 10 Руководство администратора безопасности. Sailfish.

3. При инсталляции СКЗИ должны быть обеспечены организационно-технические меры по исключению подмены дистрибутива и внесения изменений в СКЗИ после установки.

4. Исключение из программного обеспечения ПЭВМ с установленным СКЗИ средств отладки.

5. СКЗИ должно использоваться со средствами антивирусной защиты. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

6. Ключевая информация является конфиденциальной.

7. Внешняя гамма, используемая для инициализации состояния программного ДСЧ, является конфиденциальной.

8. Пароль, используемый для аутентификации пользователей, должен удовлетворять требованиям п. 15.4.

9. Периодичность тестового контроля криптографических функций - 10 минут.

10. Ежесуточная перезагрузка ПЭВМ.

11. Периодичность останова ПЭВМ с обязательной проверкой системы охлаждения процессорного блока ПЭВМ - 1 месяц.

12. Запрещается использовать режим простой замены ГОСТ 28147-89 для шифрования информации, кроме ключевой.

13. При функционировании СКЗИ должны выполняться требования эксплуатационной документации на используемый ПАК защиты от НСД.

14. Должно быть запрещено использование СКЗИ для защиты речевой информации без проведения соответствующих дополнительных исследований.

15. Должна быть запрещена работа СКЗИ при включенных в ПЭВМ штатных средствах выхода в радиоканал.

16. Контролем целостности должны быть охвачены файлы, указанные в разделах «Требования по криптографической защите» документов ЖТЯИ.00087-03 91 02, ЖТЯИ. 00087-03 91 03, ЖТЯИ.00087-03 91 04, ЖТЯИ.00087-03 91 05, ЖТЯИ.00087-03 91 06, ЖТЯИ.00087-03 91 07, ЖТЯИ.00087-03 91 08, ЖТЯИ.00087-03 91 09, ЖТЯИ.00087-03 91 10.

17. ЗАПРЕЩАЕТСЯ использование беспроводных клавиатур и компьютерных мышей.

16. Требования по встраиванию и использованию ПО СКЗИ

Встраивание СКЗИ в защищаемые информационные системы должно производиться в соответствии с Положением ПКЗ-2005. Встраивание должны проводить организации, имеющие лицензию на право проведения таких работ.

Для обеспечения защиты электронных документов и создания защищенной автоматизированной системы в первую очередь используются криптографические методы защиты, которые позволяют обеспечить защиту целостности, авторства и конфиденциальности электронной информации и реализовать их в виде программных или аппаратных средств, встраиваемых в автоматизированную систему.

При создании защищенной информационной системы должны быть определены модель возможных угроз и политика ее безопасности. В зависимости от политики безопасности определяется необходимый набор криптографических функций и организационно-технических мер, реализуемых в создаваемой системе.

Функции СКЗИ при встраивании в прикладное программное обеспечение могут быть использованы:

1. Через интерфейс функций CryptoAPI 2.0, что позволяет применять весь инструментарий фирмы Microsoft. Для этих целей разработчики могут воспользоваться программной документацией, содержащейся в MSDN (Microsoft Developer Network), а также поставляемым тестовым ПО; на Unix-платформах (Linux, FreeBSD, Solaris) через интерфейс библиотеки capilite.dll, являющейся подмножеством интерфейса CryptoAPI 2.0. Для этих целей в комплект поставки включается документ ЖТЯИ.00087-03 96 01 «КриптоПро CSP. Руководство программиста».

2. Непосредственным вызовом функций СКЗИ после загрузки модуля с использованием функции **LoadLibrary**. Для этих целей в комплект поставки включается документ ЖТЯИ.00087-03 96 01 «КриптоПро CSP. Руководство программиста», описывающий состав функций и тестовое ПО.

Защита от закладок, вирусов, модификации системного и прикладного ПО должна быть обеспечена использованием, средств антивирусной защиты и организационных мероприятий.

Правила встраивания и использования СКЗИ

При встраивании СКЗИ «КриптоПро CSP» в прикладное программное обеспечение или использовании его в составе стандартного прикладного ПО должны выполняться следующие требования:

1. При использовании открытого ключа или ключа проверки ЭП должны быть обеспечены его авторизация, достоверность, целостность и идентичность.

2. При использовании сертификатов открытых ключей и ключей проверки ЭП, заверенных подписью доверенной стороны, должна быть обеспечена безопасная доставка и хранение сертификата ключа доверенной стороны, с использованием которого проверяются остальные сертификаты ключей проверки ЭП пользователей (корневого сертификата).

3. Криптографическое средство, с помощью которого производится заверение ключей проверки ЭП, открытых ключей или справочников открытых ключей, должно быть сертифицировано по классу, соответствующему принятой политике безопасности.

4. Для отзыва (вывода из действия) открытых ключей и ключей проверки ЭП должны использоваться средства, позволяющие произвести авторизацию отзывающего лица (в этих целях должен быть использован список отозванных сертификатов, заверенный ЭП доверенной стороны).

5. При вызове Приложением функций СКЗИ в прикладном программном обеспечении должна быть предусмотрена проверка кода завершения вызываемой функции.

17.1 Требования по встраиванию модулей «КриптоПро IPSec».

С использованием модулей IPSec осуществляется защита информации при выходе в канал связи, поэтому встраивание данных модулей равноценно разработке самостоятельного СКЗИ и должно проводиться в соответствии с ПКЗ-2005.

В составе СКЗИ «КриптоПро CSP» v 4.0 R4 не все режимы модулей IPSec прошли сертификацию, это относится к режимам аутентификации GSS_API библиотеки libike_gost (cpike_api) поддержки протокола IKE и к режимам модуля esp_gost (cpesp_drv) протокола ESP. Сертификация данных режимов должна проводиться в составе разрабатываемых СКЗИ.

Литература

1. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3. ГОСТ Р 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;
4. ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
5. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
6. ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»;
7. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»;
8. Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
9. ЖТЯИ.00087-03 30 01. «КриптоПро CSP». Формуляр;
10. ЖТЯИ.00087-03 90 01. «КриптоПро CSP». Описание реализации;
11. ЖТЯИ.00087-03 91 02. «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows;
12. ЖТЯИ.00087-03 91 03. «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС в ОС Linux;
13. ЖТЯИ.00087-03 91 04. «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС FreeBSD;
14. ЖТЯИ.00087-03 91 05. «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Solaris;
15. ЖТЯИ.00087-03 91 06. «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС AIX;
16. ЖТЯИ.00087-03 91 07. «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Mac OS X;
17. ЖТЯИ.00087-03 91 08. «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС iOS;
18. ЖТЯИ.00087-03 91 09. «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ в виртуальных средах;
19. ЖТЯИ.00087-03 91 10. «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Sailfish;
20. ЖТЯИ.00087-03 92 01. СКЗИ «КриптоПро CSP». Инструкция по использованию Windows;
21. ЖТЯИ.00087-03 93 01. СКЗИ «КриптоПро CSP». АРМ выработки внешней гаммы;
22. ЖТЯИ.00087-03 96 01. «КриптоПро CSP». Руководство программиста;
23. OSI NETWORKING AND SYSTEM ASPECTS. Abstract Syntax Notation One (ASN.1);
24. ITU-T Recommendation X.509: Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, Oct 2012;
25. RFC 3280, «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», April 2002;
26. RFC 3369, «Cryptographic Message Syntax» (CMS), August 2002;
27. 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», Jan 2006.
28. RFC 4490, «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)», May 2006.
29. RFC 4491, «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.
30. Уведомление об организации перехода на использование схемы электронной подписи по ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» [Электронный ресурс]. Режим доступа: https://sc.minsvyaz.ru/media/docs/Uvedomlenie_o_plane_perehoda_GOST2012_1.pdf

Приложение А.
Акт готовности к работе.

û ú ê í ø î ì è

_____
(должность)

_____
(наименование учреждения)

_____
(подпись, ФИО)

АКТ

готовности _____ к работе с _____
(наименование учреждения) (наименования изделий)
с "_____" _____ 201___г.

Комиссия в составе председателя _____ _____ и членов,
(должность) (Ф.И.О.)
комиссии, назначенная _____ составила настоящий акт о том, что
(приказ о назначении)
помещение эксплуатирующего органа _____, размещенное _____,
(название) (адрес)
хранилища ключевых носителей, охрана помещений и подготовленность сотрудников к обслуживанию

_____
(оборудование)
соответствуют:
_____.
(ГОСТ, инструкция, руководящие документы, правила пользования и т.п.)
Комиссия отмечает, что инсталляция ПО вышеупомянутых изделий проведены в соответствии с

_____
(инструкции)
Вывод: комиссия считает, что объект_____ отвечает требованиям
название объекта
_____ _____
(название инструкции)
по обеспечению безопасности по уровню _____ и может быть введен в действие.

Председатель:

_____ _____
(подпись) (Ф.И.О)

Члены комиссии:

_____ _____
(подпись) (Ф.И.О)

_____ _____
(подпись) (Ф.И.О)

_____ _____
(подпись) (Ф.И.О)

М.П.

Приложение Б.
Журнал регистрации администраторов безопасности и пользователей

п/п	Организация	Ф.И.О. администратора безопасности пользователя системы	Данные регистрации	Дата регистрации	Дата выбытия	Примечание (пользователь, администратор)
1		Сидоров А. А.	нет	21.01.2010		Администратор безопасности
2		Иванов И. И.	Почтовый адрес: a.sidorov@acme.ru Должность:	01.02.2010		Оператор расчетной системы

Приложение В.
Журнал пользователя сети

п/п	Дата Время	Ф.И.О. пользователя системы	Событие	Дополнительные данные	Примечание

Приложение Г.
«Удостоверяющий центр «КриптоПро УЦ»

Программный комплекс «Удостоверяющий Центр «КриптоПро УЦ» предназначен для выполнения организационно-технических мероприятий по обеспечению пользователей Удостоверяющего Центра как организации средствами и спецификациями для использования сертификатов открытых ключей в целях:

– контроля целостности электронных документов, передаваемых в автоматизированных информационных системах;

– контроля целостности публичных информационных ресурсов;

– проверки подлинности взаимодействующих программных компонентов и конфиденциальности передаваемых данных при информационном взаимодействии;

– создания системы юридически значимой электронной подписи в системах электронного документооборота;

– обеспечения безопасности и разграничения доступа при взаимодействии субъектов автоматизированных информационных систем;

– создания иерархической системы управления ключами подписи субъектов автоматизированных информационных систем.

Программный комплекс «Удостоверяющий Центр «КриптоПро УЦ» обеспечивает:

– Реализацию ролевой модели управлениями объектами «КриптоПро УЦ»;

– Создание Инфраструктуры Удостоверяющих Центров, построенных по:

  ▪ иерархической модели;

  ▪ сетевой (мостовой) модели.

– Аудит событий, связанных с эксплуатацией программного комплекса;

– Реализацию механизма занесения в сертификат ключа проверки ЭП подписи сведений об отношениях, при которых электронный документ имеет юридическую силу, и областях применения сертификата;

– Ведения реестра зарегистрированных пользователей;

  ▪ Выполнение процедуры регистрации пользователя в централизованном режиме с прибытием регистрируемого пользователя в Удостоверяющий Центр;

  ▪ Выполнение процедуры регистрации пользователя в распределенном режиме без прибытия регистрируемого пользователя в Удостоверяющий Центр;

  ▪ Выполнение процедуры удаления пользователей из реестра пользователей по запросам администратора Удостоверяющего Центра;

  ▪ Выполнение процедуры удаления пользователей из реестра пользователей в автоматическом режиме;

– Генерация ключей подписи и шифрования

  ▪ Выполнение процедуры генерации личных ключей ЭП и ключей проверки ЭП и ключей шифрования пользователя на рабочем месте пользователя;

  ▪ Выполнение процедуры генерации личных ключей ЭП и ключей проверки ЭП и ключей шифрования на рабочем месте администратора Удостоверяющего Центра;

  ▪ Выполнение процедуры генерации личных ключей ЭП и ключей проверки ЭП уполномоченного лица Удостоверяющего Центра;

  ▪ Выполнение процедуры генерации личных ключей ЭП и ключей проверки ЭП уполномоченного лица подчиненного Удостоверяющего Центра;

– Ведение реестра запросов и заявлений на сертификаты открытых ключей и ключей проверки ЭП в электронном виде:

  ▪ Формирование запроса на сертификат нового ключа проверки ЭП на рабочем месте пользователя;

- Формирование запроса на сертификат нового ключа проверки ЭП на рабочем месте администратора Удостоверяющего Центра;
- Вывод запросов на сертификаты ключей проверки ЭП пользователей на бумажный носитель на рабочем месте пользователя;

– Ведение реестра сертификатов открытых ключей и ключей проверки ЭП, изданных Удостоверяющим Центром в электронном виде:

- Контроль уникальности открытых ключей шифрования и ключей проверки ЭП в формируемых сертификатах;
- Формирование сертификатов открытых ключей и ключей проверки ЭП пользователей в электронном виде в соответствии с рекомендациями X.509 версии 3 и RFC 2459, позволяющих с помощью криптографических методов (ЭП) централизованно заверять соответствие открытого ключа и ключа проверки ЭП и атрибутов определенному пользователю;
- Вывод сертификатов ключей проверки ЭП пользователей на бумажный носитель на рабочем месте пользователя;
- Вывод сертификатов ключей проверки ЭП пользователей на бумажный носитель на рабочем месте администратора Удостоверяющего Центра;

– Ведение реестра запросов и заявлений на аннулирование (отзыв) и приостановление/возобновления действия сертификатов открытых ключей и ключей проверки ЭП в электронном виде:

- Выполнение процедуры формирования запросов на отзыв сертификатов ключей проверки ЭП на рабочем месте пользователя;
- Выполнение процедуры формирования запросов на отзыв сертификатов ключей проверки ЭП пользователей на рабочем месте администратора Удостоверяющего Центра;
- Выполнение процедуры формирования запросов от пользователей на приостановление/возобновление действия сертификатов ключей проверки ЭП на рабочем месте пользователя;
- Выполнение процедуры формирования запросов на приостановление/возобновление действия сертификатов ключей проверки ЭП пользователей на рабочем месте администратора Удостоверяющего Центра;
- Формирование и доставку зарегистрированным пользователям списка отозванных сертификатов ключей проверки ЭП пользователей;

– Выполнение процедуры подтверждения подлинности ЭП:

- Выполнение процедуры подтверждения подлинности ЭП в электронных документах;
- Выполнение процедуры подтверждения подлинности ЭП уполномоченного лица Удостоверяющего Центра в изданных сертификатах ключей проверки ЭП;

– Реализацию системы оповещения пользователей с использованием почтовых сообщений:

- Управление оповещением пользователей о событиях в процессе регистрации;
- Управление оповещением пользователей о событиях в течении всего жизненного цикла сертификатов ключей проверки ЭП.

Архитектура ПК «КриптоПро УЦ»

Программный комплекс «Удостоверяющий центр «КриптоПро УЦ» состоит из следующих компонент:

– Центр Сертификации (ЦС);

– Центр Регистрации (ЦР);

- АРМ администратора ЦР;
- АРМ разбора конфликтных ситуаций;
- Пользовательских средств взаимодействия с УЦ;
  - АРМ регистрации пользователя;
  - АРМ зарегистрированного пользователя с маркерным доступом;
  - АРМ зарегистрированного пользователя с ключевым доступом.
- Программного интерфейса взаимодействия с УЦ (Интерфейс Внешних Приложений).

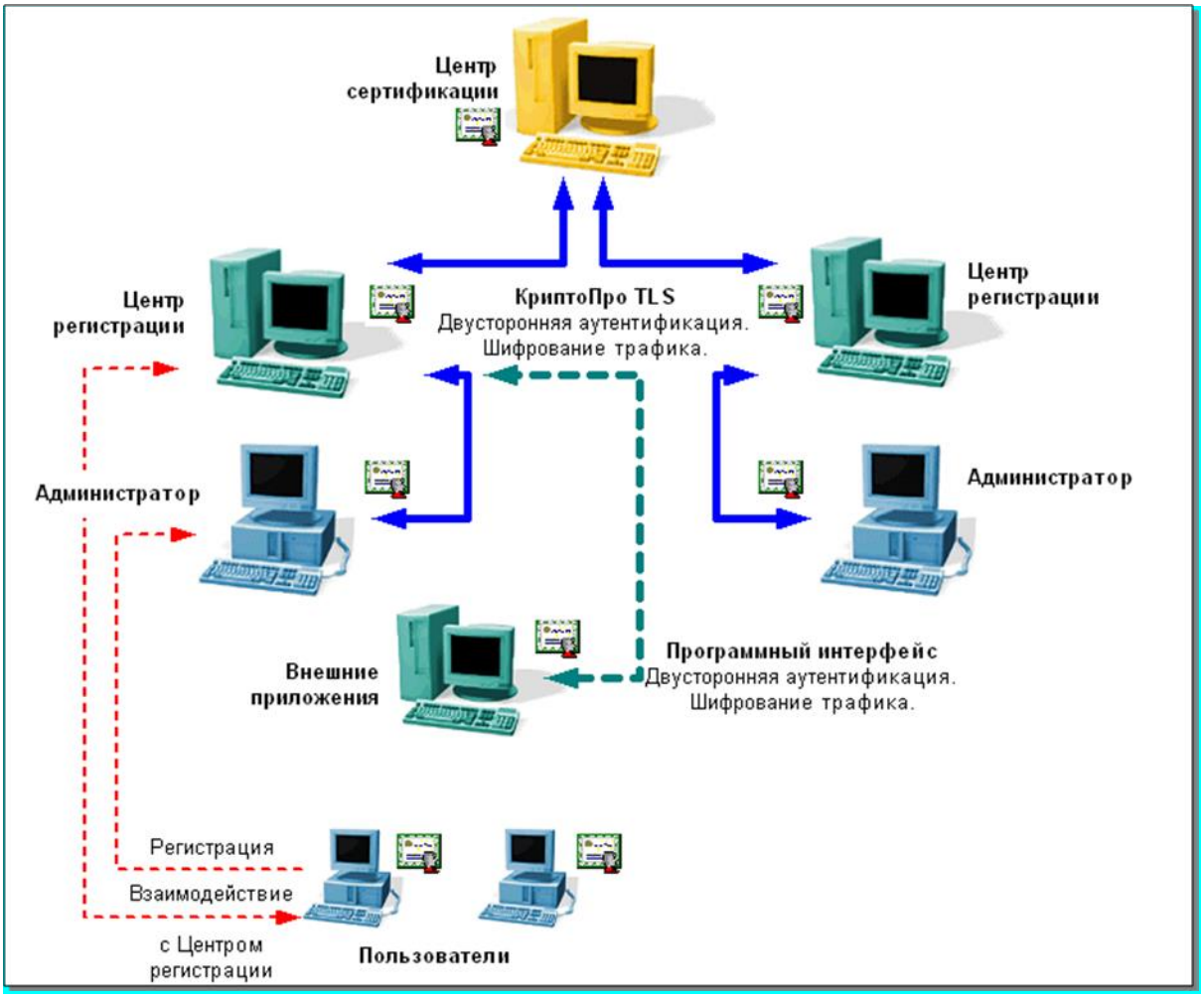


Рисунок Г1 – Схема взаимодейтсвия компонент «КриптоПро УЦ»

Центр Сертификации

Центр сертификации – компонент комплекса «КриптоПро УЦ», предназначенный для формирования сертификатов ключей проверки ЭП пользователей и администраторов Удостоверяющего центра, списков отозванных сертификатов, хранения эталонной базы сертификатов и списков отозванных сертификатов. Центр Сертификации функционирует в операционной системе (ОС) Microsoft Windows Server 2003/2008 R2/2012/2012 R2 и использует базу данных Microsoft SQL Server 2005 Express (по умолчанию) (MSSE) и базу данных службы сертификации Microsoft Certificate Authority (CA). MSSE устанавливается программой установки ПО Центра Сертификации и не требует отдельной установки.

В качестве системы управления базой данных Центра Сертификации может использоваться Microsoft SQL Server 2005, Microsoft SQL Server 2008 (с установленным пакетом совместимости с SQL 2005), Microsoft SQL Server 2008 R2 (с установленным пакетом

совместимости с SQL 2005), Microsoft SQL Server 2012 (с установленным пакетом совместимости с SQL 2005).

ЦС взаимодействует только с Центром Регистрации или несколькими Центрами Регистрации по отдельному сегменту локальной сети с использованием защищенного сетевого протокола.

Центр регистрации

Центр Регистрации – компонент ПК «КриптоПро УЦ», предназначенный для хранения регистрационных данных пользователей, запросов на сертификаты и сертификаты пользователей, предоставления интерфейса взаимодействия пользователей с Удостоверяющим Центром. Центр Регистрации функционирует в операционной системе (ОС) Microsoft Windows Server 2003/2008 R2/2012/2012 R2 и использует базу данных Microsoft SQL Server 2005 Express (MSSE) (по умолчанию). MSSE устанавливается программой установки ПО Центра Регистрации.

Центр Регистрации взаимодействует с Центром Сертификации по отдельному сегменту локальной сети с использованием защищенного сетевого протокола. Взаимодействие пользователей с Удостоверяющим центром обеспечивается за счет использования приложений (АРМ зарегистрированного пользователя с ключевым доступом, АРМ зарегистрированного пользователя с маркерным доступом, АРМ регистрации пользователя), предоставляемых Центром Регистрации.

Центр Регистрации является единственной точкой входа (регистрации) пользователей в системе. Только зарегистрированный в Центре Регистрации пользователь может получить сертификат на свой открытый ключ в Удостоверяющем Центре.

АРМ администратора ЦР

Компонент АРМ Администратора ЦР предназначен для выполнения организационно-технических мероприятий, связанных с регистрацией пользователей, формированием служебных ключей и сертификатов пользователей и управления Центром регистрации. АРМ администратора функционирует в ОС Microsoft Windows 7/8/8.1/10. АРМ администратора взаимодействует с Центром Регистрации по локальной сети с использованием защищенного сетевого протокола.

Программное обеспечение АРМа администратора является универсальным и используется для всех ролей привилегированных пользователей (администраторов, операторов и т.д.).

АРМ разбора конфликтных ситуаций

АРМ разбора конфликтных ситуаций предназначен для выполнения организационно-технических мероприятий, связанных:

– с подтверждением подлинности ЭП в электронных документах и определения статуса сертификатов открытых ключей пользователей;

– с подтверждением подлинности ЭП уполномоченного лица Удостоверяющего Центра в изготовленных им сертификатах открытых ключей.

АРМ разбора конфликтных ситуаций функционирует в ОС Microsoft Windows 7/8/8.1/10. АРМ разбора конфликтных ситуаций не взаимодействует ни с каким другим компонентом Удостоверяющего Центра и использует в своей работе объекты, предъявляемые сторонами конфликта в качестве доказательства тех или иных фактов (электронный документ с ЭП, сертификаты, списки отозванных сертификатов и т.д.).

АРМ регистрации пользователя.

АРМ регистрации пользователя Центра Регистрации предназначен для выполнения организационно-технических мероприятий, связанных с выполнением процедуры регистрации пользователя на Удостоверяющем Центре в режиме распределенной регистрации.

АРМ регистрации пользователя функционирует в ОС Microsoft Windows (с установленным MS IE 5.0 и выше). АРМ регистрации пользователя взаимодействует с Центром регистрации по протоколу HTTP(S) с односторонней аутентификацией.

К основным функциям АРМ регистрации пользователя относятся:

– обеспечение взаимодействия с Центром Регистрации;

– обеспечение возможности формирования и передачи запроса на регистрацию пользователя;

– шифрование информации, передаваемой между пользователем и Центром Регистрации, с использованием протокола TLS с односторонней аутентификацией.

АРМ зарегистрированного пользователя с маркерным доступом.

АРМ зарегистрированного пользователя с маркерным доступом предназначен для выполнения организационно-технических мероприятий, связанных с генерацией служебных ключей, формированием запроса на служебный сертификат ключа проверки ЭП и получение служебного сертификата ключа проверки ЭП.

Аутентификация зарегистрированного пользователя осуществляется с использованием временного маркера доступа, представляющего собой совокупность следующих сущностей:

– Идентификатор (ID);

– Пароль.

Идентификатор формируется Центром Регистрации и представляет собой целое число.

Пароль формируется Центром Регистрации и представляет собой строку символов длиной 6.

Маркер доступа, сформированный Центром Регистрации, передается пользователю либо в процессе регистрации (с использованием АРМ заочной (удаленной) регистрации) по защищенному каналу, либо сообщается пользователю администратором.

АРМ зарегистрированного пользователя с маркерным доступом, как правило, используется в двух случаях:

– в процедуре распределенной регистрации пользователя, после использования АРМ регистрации пользователя;

– в случае потери ключа аутентификации (при компрометации или в иных случаях) зарегистрированного пользователя и не имеющего возможности личного прибытия в Удостоверяющий Центр для получения ключей и сертификатов.

АРМ зарегистрированного пользователя с маркерным доступом функционирует в ОС Microsoft Windows 7/8/8.1/10 (с установленным MS IE 5.0 и выше). АРМ зарегистрированного пользователя с маркерным доступом взаимодействует с Центром регистрации по протоколу HTTP(S) с односторонней (серверной) аутентификацией.

АРМ зарегистрированного пользователя с ключевым доступом.

АРМ зарегистрированного пользователя с ключевым доступом предназначен для выполнения организационно-технических мероприятий, связанных с управлением личной ключевой информацией и сертификатами, такими как формирование рабочих ключей и заявлений на изготовление сертификатов, заявлений на аннулирование сертификатов, приостановление и возобновления действия, получение и установка списка отозванных сертификатов.

АРМ зарегистрированного пользователя с ключевым доступом функционирует в ОС Microsoft Windows 7/8/8.1/10 (с установленным MS IE 5.0 и выше). АРМ зарегистрированного пользователя с ключевым доступом взаимодействует с Центром регистрации по протоколу HTTP(S) с двухсторонней аутентификацией.

Интерфейс Внешних Приложений «КриптоПро УЦ»

Программное обеспечение Центра Регистрации реализовано в виде веб-сервиса. Веб-сервис Центра Регистрации базируются на трех основных веб-стандартах:

– SOAP (Simple Object Access Protocol) —протокол для посылки сообщений по протоколу HTTP(HTTPS) и другим Internet-протоколам;

– WSDL (Web Services Description Language) — на языке для описания программных интерфейсов веб-сервисов;

– UDDI (Universal Description, Discovery and Integration) — на стандарте для индексации веб-сервисов.

Например, консоль администратора Центра Регистрации общается с сервером приложения путем вызова методов удаленных объектов по SOAP протоколу, используя WSDL описание веб-сервиса RA.wsdl.

Центр регистрации предоставляет программный интерфейс внешних приложений (ИВП) для доступа к функциональности ЦР. Программный интерфейс используется внешними приложениями, которые могут выступать в роли пользователя или администратора, в зависимости от предоставляемого сертификата.

Для обеспечения вызовов удаленных объектов с использованием SOAP протокола Центр Регистрации содержит специальную ASP страницу «RA.asp» — обработчик SOAP-запросов. Этот обработчик принимает SOAP запросы, поступающие по протоколам HTTP или HTTPS, в виде документов XML. С использованием WSDL и WSML описания веб-сервиса, он преобразует их в вызовы объектов приложения COM+ Центра Регистрации. По окончанию вызова, он получает возвращаемые значения, упаковывает их в SOAP сообщение и отправляет его клиентской части приложения.

Фактически, разработка приложения, которому необходима функциональность Центра Регистрации, сводится к написанию программы, которая формирует «правильные», в соответствии с WSDL описанием, SOAP запросы, содержащие название веб-сервиса, порта, вызываемого метода, наименования и значения параметров метода. Потом некоторым образом эта программа отправляет их по протоколам HTTP или HTTPS на URL адрес RA.asp. В ответ эта программа получает SOAP ответ с результатами вызова, затем разбирает этот пакет и извлекает возвращаемые значения.

Режимы работы «КриптоПро УЦ»

1) Режимы регистрации пользователей Удостоверяющего Центра

ПК «КриптоПро УЦ» обеспечивает реализацию следующих режимов регистрации пользователей:

– Централизованный режим

При централизованном режиме регистрации, идентификация пользователя осуществляется администратором Удостоверяющего Центра на основании документов, удостоверяющих личность пользователя, при личном прибытии регистрируемого пользователя в УЦ.

Администратор с использованием ПО АРМ администратора Центра Регистрации формирует запрос на регистрацию в электронной форме от имени пользователя и принимает его.

– Распределенный режим

Распределенный режим регистрации пользователя является опциональным режимом и используется при невозможности (по разным причинам, в том числе и по причине экономической целесообразности) регистрации пользователей в централизованном режиме.

Идентификация пользователя осуществляется нотариусом путем совершения нотариальных действий при заверении заявления на регистрацию пользователя, на основании документов, удостоверяющих личность пользователя.

С помощью ПО АРМ регистрации пользователя регистрируемые пользователи формируют запрос на регистрацию в электронной форме.

Регистрация пользователя в распределенном режиме на УЦ осуществляется администратором Удостоверяющего Центра на основании нотариально заверенного заявления на регистрацию и запроса на регистрацию в электронной форме путем принятия запроса на регистрацию в электронной форме.

2) Режимы управления ключами и сертификатами открытых ключей пользователей Удостоверяющего Центра

– Централизованный режим

Пользователи УЦ получают ключи и сертификаты открытых ключей у ответственного сотрудника (администратора) УЦ.

Администратор выполняет процедуры генерации ключей и сертификатов пользователей на своем рабочем месте с использованием ПО АРМ администратора Центра Регистрации.

Управление сертификатами пользователей в течении их жизненного цикла, также осуществляется администратором УЦ.

– Распределенный режим

Пользователи Удостоверяющего Центра самостоятельно осуществляют процедуру генерации ключей и формирование запросов на сертификат открытого ключа.

Выполнение этих процедур осуществляется с использованием АРМ зарегистрированного пользователя на рабочем месте.

Поступающие запросы на сертификаты открытых ключей пользователей обрабатываются администратором УЦ с использованием АРМ администратора Центра Регистрации.

Установку на рабочем месте выпущенных сертификатов открытых ключей пользователь осуществляет также с использованием АРМ зарегистрированного пользователя. На АРМ зарегистрированного пользователя предоставляется возможность осуществить формирование запроса на отзыв (приостановление/возобновление действия) сертификатов открытых ключей и ключей проверки ЭП.

Масштабируемость и производительность ПК «КриптоПро УЦ»

Масштабируемость

Наличие в составе программного обеспечения Центра Регистрации программного интерфейса для работы с внешними приложениями третьих фирм позволяет создавать интегрированные решения.

Программный интерфейс предоставляет возможность встроить в сторонние программные продукты функции по управлению объектами Центра Регистрации (учетные записи пользователей, сертификаты, запросы от пользователей и т.д.). Такое встраивание позволяет оптимизировать информационные потоки в прикладных системах за счет совмещения регистрации пользователей в прикладной системе с регистрацией пользователя на Удостоверяющем Центре, упрощения авторизации абонентов в системах защищенного документооборота и так далее.

Реализация программного интерфейса Центра Регистрации с использованием защищенного транспортного протокола TLS и строгой аутентификации взаимодействующих компонентов на основе сертификатов открытых ключей, обеспечивает авторизацию клиентских и серверных частей интегрированного приложения и обеспечивает конфиденциальность передаваемых данных. Требование обеспечения конфиденциальности передаваемых данных между внешним приложением и Центром Регистрации возникает в следствии того, что в состав передаваемых данных входит и персональная информация пользователей, и информация из документов, регламентирующих обслуживание пользователя в прикладной системе.

Поддержка нескольких Центров Регистрации в составе одного комплекса Удостоверяющего Центра становится актуальна в случае наличия различных бизнес-моделей управления регистрационными записями пользователей и их ключевой информации в прикладных системах предприятия. Изменяя настройки и режимы работы в Центрах Регистрации, обслуживающих соответствующие прикладные системы, в соответствии с

предъявляемыми требованиями достигается оптимизация системы управления учетной информации пользователей, ключами и сертификатов открытых ключей и ключей проверки ЭП.

Рисунок Г2 – Поддержка нескольких ЦР

Взаимодействие компонент Удостоверяющего Центра посредством защищенных соединений с использованием протокола HTTP(S) обеспечивает территориально-распределенную модель Удостоверяющего Центра. Использование в качестве системы телекоммуникаций сеть Интернет позволяет значительно удешевить реализацию такой модели Удостоверяющего Центра без существенного ослабления требований по безопасности.

Производительность

С целью проведения независимой экспертизы потребительских свойств и производительности ПК «КриптоПро УЦ», ООО "КРИПТО-ПРО" (http://www.cryptopro.ru) и ЗАО "Удостоверяющий Центр" (http://www.nwudc.ru/) заключили соглашение, в рамках которого на технологической базе ЗАО "Удостоверяющий Центр" силами специалистов компании были проведены испытания ПАК «КриптоПро УЦ». Программа и методика испытаний была разработана совместно специалистами ООО "КРИПТО-ПРО" и ЗАО "Удостоверяющий Центр" и предусматривала выполнение тестов, подтверждающих функциональные возможности ПАК «КриптоПро УЦ», заявленных производителем. Также в рамках этих договоренностей выполнялись нагрузочные тесты по регистрации пользователей на «КриптоПро УЦ».