127 018, Москва, Улица Образцова, 38
Телефон: (095) 933 1168
Факс: (095) 933 1168
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро CSP

Версия 3.0

Руководство администратора безопасности

Общая часть

ЖТЯИ.00003-01 90 02
Листов 74

2005 г.

© ООО "Крипто-Про", 2000-2005. Все права защищены.

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

Документ входит в комплект поставки программного обеспечения КриптоПро CSP, и 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

Аннотация 6
1. Список сокращений 7
2. Основные термины и положения 7
3. Основные технические данные и характеристики СКЗИ 20
3.1. Операционные системы 21
3.2. Исполнения 21
3.3. Реализуемые алгоритмы 21
3.4. Ключевые носители 22
3.5. Размеры ключей 22
4. Архитектура ПО и общие принципы функционирования 22
4.1. Состав программного обеспечения 23
4.2. СКЗИ КриптоПро CSP 25
4.3. ПКЗИ КриптоПро CSP 25
5. Описание протокола сетевой аутентификации КриптоПро TLS 25
5.1. Назначение протокола TLS 25
5.2. Основные понятия протокола TLS 26
5.3. Модуль поддержки сетевой аутентификации КриптоПро TLS 29
6. Ключевая система и ключевые носители 31
6.1. Общие положения 31
6.1.1. Шифрование данных 31
6.1.2. Формирование и проверка ЭЦП 31
6.2. Ключевой контейнер 31
6.3. Структура ключевого контейнера 32
6.4. Формирование ключей 32
6.5. Хранение ключевых носителей 33
6.6. Сроки действия ключей 33
6.7. Уничтожение ключей на ключевых носителях 33
6.8. Интерфейс управления ключами СКЗИ 33
7. Рекомендации по встраиванию и использованию ПО СКЗИ 33
7.1. Конфиденциальность информации 34
7.2. Идентификация и авторство 34
7.3. Целостность 34
7.4. Неотказуемость от передачи электронного документа 35
7.5. Неотказуемость от приема электронного документа 35
7.6. Защита от переповторов 35
7.7. Защита от навязывания информации 35
7.8. Защита от закладок, вирусов, модификации системного и прикладного ПО 35

7.9. Правила встраивания и использования СКЗИ КриптоПро CSP 35
8. Управление ключами СКЗИ 36
8.1. Удостоверяющий центр 37
8.2. Формирование ключей Центра Сертификации 38
8.2.1. Закрытый ключ и сертификат ЦС 38
8.3. Хранение и использование закрытого ключа ЦС 38
8.4. Формирование ключей Центра Регистрации 38
8.4.1. Регистрация Центра Регистрации 38
8.4.2. Ключ и сертификат ЦР 39
8.4.3. Изготовление ключей Центра Регистрации 39
8.5. Формирование ключей пользователя 39
8.5.1. Регистрация пользователя 40
8.5.2. Ключ и сертификат пользователя 40
8.5.3. Формирование личных ключей пользователя 41
8.5.4. Получение личного сертификата пользователем 41
8.6. Повторная регистрация пользователя 41
8.7. Плановая смена ключей 42
8.7.1. Смена ключей Центра Сертификации 42
8.7.2. Смена ключей Центра Регистрации 42
8.7.3. Смена ключей пользователя 42
8.8. Компрометация ключей 42
8.8.1. Компрометация ключей Центра Сертификации 42
8.8.2. Компрометация ключей Центра Регистрации 43
8.8.3. Компрометация ключей пользователя 43
8.8.4. Действия УЦ при компрометации ключей пользователя 43
8.9. Исключение пользователя из сети 44
8.10. Периодичность издания СОС 44
8.11. Ведение журналов 44
9. Порядок разбора конфликтных ситуаций, связанных с применением ЭЦП 45
9.1. Порядок разбора конфликтной ситуации 45
9.2. Случаи невозможности проверки значения ЭЦП 46
10. Нештатные ситуации при эксплуатации СКЗИ 47
11. Рекомендации по размещению технических средств с СКЗИ . 48
12. Рекомендации по установке ПО СКЗИ на ПЭВМ 49
13. Требования по защите от НСД 49
13.1. Принципы защиты информации от НСД 50
13.2. Организационные меры защиты информации от НСД 50
13.3. Средства защиты от НСД, применяемые в СКЗИ КриптоПро CSP 52
13.3.1. Программно-аппаратный комплекс "Аккорд-АМДЗ" 52
13.3.2. Электронный замок "Соболь" 52

14. Обеспечение безопасности функционирования рабочих мест со встроенными средствами криптографической защиты..... 53

Литература 55

Приложение 1. Акт готовности к работе..... 57

Приложение 2. Журнал регистрации администраторов безопасности и пользователей..... 58

Приложение 3. Журнал пользователя сети..... 58

Приложение 4. ПК «Удостоверяющий центр «КриптоПро УЦ» 59

Индекс 67

Аннотация

Настоящее руководство содержит общее описание средства криптографической защиты информации (СКЗИ) КриптоПро CSP v. 3.0, его состав, ключевую систему, рекомендации по размещению технических средств, использующих СКЗИ, рекомендации по проверке целостности установленного ПО СКЗИ, по использованию СКЗИ в различных автоматизированных системах и средствах вычислительной техники.

В зависимости от исполнения СКЗИ настоящее Руководство дополняется следующими документами:

- ЖТЯИ.00015-01 90 02-01. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows 2000/XP/2003.

- ЖТЯИ.00015-01 90 02-02. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Red Hat Linux 7, 9.

- ЖТЯИ.00015-01 90 02-03. Руководство администратора безопасности. Использование СКЗИ под управлением ОС FreeBSD 5.

- ЖТЯИ.00015-01 90 02-04. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Solaris 9 Update 4.

- ЖТЯИ.00015-01 90 02-05. Инструкция по использованию КриптоПро CSP и TLS.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ КриптоПро CSP, должны разрабатываться с учетом требований настоящего Руководства.

1. Список сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
ITU-T	Международный комитет по телекоммуникациям (International Telecommunication Union)
IETF	Internet Engineering Task Force
TM	Устройство хранения информации на таблетке touch-memory
АС	Автоматизированная система
АРМ	Автоматизированное рабочее место
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск
КП	Конечный пользователь
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПКЗИ	Подсистема криптографической защиты информации
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.
СВТ	Средства вычислительной техники
Сертификат	Электронный документ, подтверждающий принадлежность открытого *ключа* и определенных *атрибутов* конкретному абоненту
Сертификация	Процесс изготовления *сертификата* открытого ключа абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей. Сетевой справочник.
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ЭД	Электронный документ
ЭЦП	Электронная цифровая подпись

2. Основные термины и положения

Автоматизированная информационная система

Комплекс программных и технических средств, предназначенных для сбора, хранения, поиска и выдачи информации по запросам [27].

Автоматизированная система

Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [10].

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:

1. контроль целостности программного обеспечения;
2. управление ключевой системой: хранение, ввод в действие и смена ключей пользователей, генерация закрытых и открытых ключей подписи пользователей;
3. 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 [20].

Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности [20].

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 [26].

Безопасность

4. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз [3].
5. Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба [16].

Безопасность информации (информационная безопасность)

1. 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. [19].

2. Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз [20].

Блокирование информации

Прекращение или затруднение доступа законных пользователей к информации [21].

Верификация

1. Установление соответствия принятой и переданной информации с помощью логических методов [25].
2. процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие [20].

Владелец информации

1. Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации [18].
2. Субъект информационных отношений, обладающий правом владения, распоряжения и пользованием информационным ресурсом по договору с собственником информации [28].

Владелец информации, информационной системы

Субъект, в непосредственном ведении которого в соответствии с законом находятся информация, информационная структура [1].

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 [2].

Гриф конфиденциальности

Специальная отметка на носителе информации либо в сопроводительных документах на него, свидетельствующая о том, что носитель содержит конфиденциальную информацию [25].

Гриф секретности

Реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и/или в сопроводительной документации на него [2].

Документ

1. Документированная информация, снабженная определенными реквизитами [1].
2. Материальный объект с информацией, закрепленной созданным человеком способом для ее передачи во времени и пространстве [17].

Документированная информация (документ)

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

Примечание. Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную [1].

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 задокументированную 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 цифровой 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

1. Получение субъектом возможности ознакомления с информацией, в том числе с помощью технических средств [18].
2. Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации [20].

Доступность информации

Свойство информации, технических средств и технологии обработки, характеризующееся способностью обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия [21].

Заверение (нотаризация)

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

Защита информации

1. Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [18].
2. Комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации [19].

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 [23].

Защищенное средство вычислительной техники (защищенная автоматизированная система)

Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты [20].

IA32

Аппаратная платформа, поддерживающая 32-разрядную архитектуру Intel.

IA64

Аппаратная платформа, поддерживающая 64-разрядную архитектуру Intel.

SPARC

Аппаратная платформа, поддерживающая архитектуру Sun Sparc.

Идентификация

Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов [20].

Имитозащита

Защита системы шифрованной связи от навязывания ложных данных [11].

Имитовставка

Отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты [11].

Ключ (криптографический ключ)

Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований [11].

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)

Различают два вида компрометации закрытого ключа: **явную** и **неявную**. Первые четыре события должны трактоваться как явная компрометация ключей. Три следующих события 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

1. Документированная информация, доступ к которой ограничивается в соответствии с Законодательством РФ [1].
2. Информация, требующая защиты [20].

Контроль доступа (управление доступом)

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

Криптографическая защита

Защита данных при помощи криптографического преобразования данных [11].

Криптопровайдер

Криптопровайдер реализован как библиотека, динамически загружаемая в единое адресное пространство процесса, инициируемого прикладной задачей. 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 ЭЦП и обмена, ввод ключей с ключевых носителей, защищённое хранение и уничтожение ключей в оперативной памяти.

Криптопродрайвер

Криптодрайвер загружается в адресное пространство ядра ОС. Реализует функции шифрования и вычисления имитовставки, хэширования и проверки подписи. Обеспечивает работу с сессионными ключами шифрования (генерация, экспорт/импорт в защищенном виде), открытыми ключами ЭЦП, эфемерными закрытыми и открытыми ключами обмена, защищённое хранение и уничтожение ключей в оперативной памяти.

По своему интерфейсу и функциональным возможностям криптодрайвер обеспечивает возможности криптопровайдера за исключением функций формирования цифровой подписи, работы с носителем ключей, генерации ключей пользователя. Криптодрайвер 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

Криптосервис реализован как 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 данных при помощи шифрования и (или) выработки имитовставки [11].

Лицензирование в области защиты информации

Деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации [19].

Мероприятия по защите информации

Совокупность действий по разработке и/или практическому применению способов и средств защиты информации [18].

Мероприятия по контролю эффективности защиты информации

Совокупность действий по разработке и/или практическому применению способов и средств контроля эффективности защиты информации [18].

Метка конфиденциальности

Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте [20].

Нарушитель безопасности информации

Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами [21].

Нарушитель правил разграничения доступа

Субъект доступа, осуществляющий несанкционированный доступ к информации [20].

Некорректный электронный документ

Электронный документ, не прошедший процедуры расшифрования данных, проверки электронной цифровой 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 информацией, 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 [18].

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 [18].

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 [18]
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) [20] [22].

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 [18].

Объект доступа

Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа [20].

Объект защиты

1. Информация или носитель информации, или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации [18].
2. Информация, технические средства и технология ее обработки, в отношении которых необходимо обеспечить безопасность информации [21].

Обработка информации

Передача, прием, хранение, преобразование и отображение информации.

Организация защиты информации

Содержание и порядок действий по обеспечению защиты информации [18].

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 цифровой 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 [20].
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 [21].
2. Нежелательные излучения и наводки, проявляющиеся в виде побочных, внеполосных, шумовых и наводимых сигналов, потенциально образующих неконтролируемые каналы утечки конфиденциальной информации [25].

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 [28].

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 [1].

Пользователь (потребитель) информации

1. Субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею [1].
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 [18].

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 [18].

Правила разграничения доступа (ПРД)

Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа [20].

Право доступа к защищаемой информации; право

Совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации [18].

Проверка электронной подписи документа

Проверка соотношения, связывающего хэш-функцию документа, подпись под этим документом и открытый ключ 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 информации

Несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к этой информации [18].

Расшифрование данных

Процесс преобразования зашифрованных данных в открытые данные при помощи шифра [11].

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 [25].

Санкционированный доступ к информации

Доступ к информации, не нарушающий правила разграничения доступа [20].

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 [20].

Сертификат открытого ключа

Сертификат открытого ключа 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;
- ЭЦП Издателя (Удостоверяющего центра), заверяющую совокупность этих данных.

Формат сертификата определен в рекомендациях ITU-T 1997 года X.509 [X.509] и рекомендациях IETF 1999 года RFC 2459 [PKIX]. 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 [5].

Секретный (закрытый) ключ

Криптографический ключ, который хранится пользователем системы в тайне. Он используется для формирования электронной цифровой подписи и 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 [18].

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 [20].

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 [9].
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 [9].

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 [28].
2. Субъект, в полном объеме реализующий полномочия владения, пользования и распоряжения информацией в соответствии с законодательными актами [18].
3. Юридическое или физическое лицо, владеющее информацией в соответствии с Законом о собственности [21].

Способ защиты информации

Порядок и правила применения определенных принципов и средств защиты информации [18].

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 [25].

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 [22].

Средства вычислительной техники

Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем [24].

Средство защиты информации

Техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации [18].

Средство защиты от несанкционированного доступа

Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа [20].

Средство криптографической защиты информации

Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности [20].

Субъект доступа

Лицо или процесс, действия которого регламентируются правилами разграничения доступа [20].

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 [28].

Техническое средство обработки информации

Техническое средство, предназначенное для приема, накопления, хранения, поиска, преобразования, отображения и передачи информации по каналам связи [19].

Угроза безопасности

Совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства [3].

Удостоверяющий центр

Центр управления открытыми ключами в соответствии с рекомендациями X509 в части использования сертификатов открытых ключей.

Уничтожение информации

Действие, в результате которого информация перестает физически существовать в технических средствах ее обработки [21].

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 [18].
2. Неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация доверена [25].

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 цифровой подписи для сокращения времени подписи и проверки подписи. Эффект сокращения времени достигается за счет вычисления подписи только под образом подписываемого набора данных [12].

Целостность информации

1. Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения) [20].
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 [18].
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 [1].

Шифр

Совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей [11].

Шифрование

Процесс зашифрования или расшифрования [11].

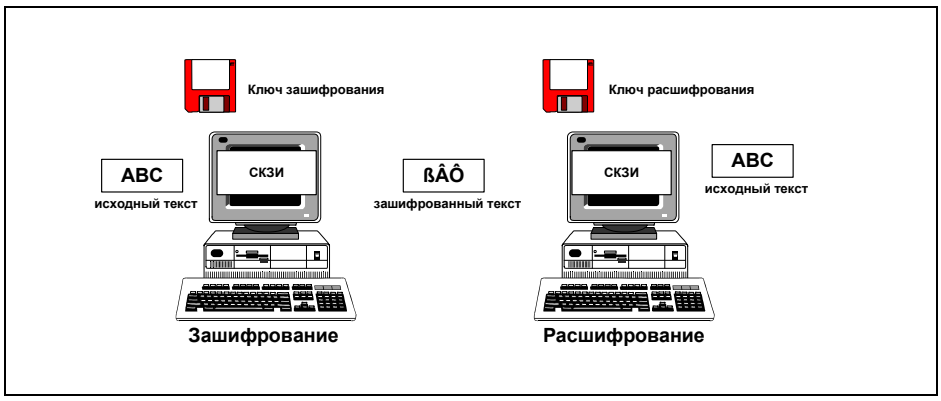


Рис. 1. Шифрование информации

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

Средства криптографической защиты информации:

1. реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации (в том числе и входящие в системы и комплексы защиты информации от несанкционированного доступа), циркулирующей в технических средствах, при ее обработке, хранении и передаче по каналам связи, включая шифровальную технику;
2. реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной цифровой подписи";
3. аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для изготовления и распределения ключевых документов, используемых в шифровальных средствах, независимо от вида носителя ключевой информации. [19]
4. ручные шифры, документы кодирования и другие носители ключевой информации.

Электронная цифровая 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 так же обеспечить защиту от подлога со стороны приемника данных.

Проверка электронной цифровой подписи под блоком открытой информации производится с помощью криптографического преобразования и открытого ключа, соответствующего закрытому, участвовавшего в процессе установки ЭЦП.



Рис. 2. Формирование и проверка ЭЦП

Электронная цифровая 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 цифровая 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, закрытым и открытым ключами.

Практическая невозможность подделки электронной цифровой 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.

3. Основные технические данные и характеристики СКЗИ

СКЗИ КриптоПро CSP версии 3.0 является модификацией СКЗИ КриптоПро CSP версии 2.0, совместимо с ним по выполняемым криптографическим функциям и отличается расширением программно-аппаратных сред функционирования. КриптоПро CSP 3.0 так же совместимо с КриптоПро CSP версии 1.1.

СКЗИ КриптоПро CSP версии 3.0 выпускается в 10 исполнениях, отличающихся программно-аппаратной средой функционирования, составом программных модулей и классом защиты (КС1, КС2) «Требований к средствам криптографической защиты конфиденциальной информации».

СКЗИ КриптоПро CSP версии 3.0 по сравнению с предыдущими версиями расширяет возможности пользователей по управлению ключами, имеет в своем составе реализацию в форме драйвера ядра операционной системы.

СКЗИ КриптоПро CSP версии 3.0 предназначено для защиты конфиденциальной информации.

Средствами СКЗИ КриптоПро CSP НЕ ДОПУСКАЕТСЯ защищать информацию, составляющую государственную тайну.

3.1. Операционные системы

СКЗИ КриптоПро CSP функционирует в следующих операционных системах (ОС):

- Windows 2000 (платформа IA32);
- Windows XP (платформа IA32);
- Windows 2003 (платформа IA32);
- Windows XP (платформа IA64);
- Windows 2003 (платформа IA64);
- Red Hat Linux 7 (платформа IA32);
- Red Hat Linux 9 (платформа IA32);
- FreeBSD 5 (платформа IA32);
- Solaris 9 Update 4 (платформа IA32);
- Solaris 9 Update 4 (платформа SPARC).

3.2. Исполнения

Исполнения 1-5 СКЗИ в составе криптопровайдера в форме подгружаемой динамической библиотеки, криптодрайвера, модуля сетевой аутентификации (TLS) и сервисных программ удовлетворяют требованиям защиты по классу **КС1** и функционируют в программно-аппаратных средах:

- Исполнение 1 – ОС Windows 2000/XP/2003 (платформы IA32, IA64);
- Исполнение 2 – ОС Red Hat Linux 7 (платформа IA32);
- Исполнение 3 – ОС Red Hat Linux 9 (платформа IA32);
- Исполнение 4 – ОС FreeBSD 5 (платформа IA32);
- Исполнение 5 – ОС Solaris 9 Update 4 (платформы SPARK, IA32);

Исполнения 6-10 СКЗИ в составе криптопровайдера в форме сервиса хранения ключей, криптодрайвера, модуля сетевой аутентификации (TLS) и сервисных программ удовлетворяют требованиям защиты по классу **КС2** и функционируют в программно-аппаратных средах:

- Исполнение 6 – ОС Windows 2000/XP/2003 (платформы IA32);
- Исполнение 7 – ОС Red Hat Linux 7 (платформа IA32);
- Исполнение 8 – ОС Red Hat Linux 9 (платформа IA32);
- Исполнение 9 – ОС FreeBSD 5 (платформа IA32);
- Исполнение 10 – ОС Solaris 9 Update 4 (платформы SPARK, IA32);

Исполнения 6-9 и исполнение 10 для аппаратно-программной среды ОС Solaris 9 Update 4 (платформа IA32) комплектуются аппаратными средствами защиты от НСД (см. «Средства защиты от НСД, применяемые в СКЗИ КриптоПро CSP»).

3.3. Реализуемые алгоритмы

Алгоритм зашифрования/расшифрования данных и вычисление имитовставки реализован в соответствии с требованиями ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая".

Алгоритмы формирования и проверки ЭЦП реализованы в соответствии с ГОСТ Р 34.10-94 "Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма" и ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".

Примечание. Организационно-техническими мерами должна быть исключена возможность использования алгоритма ГОСТ Р 34.10-94 *для вычисления электронной цифровой подписи после 31.12.2007 г.*

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

Ключевая система СКЗИ КриптоПро CSP обеспечивает возможность парно-выборочной связи абонентов сети с использованием для каждой пары абонентов уникальных ключей, создаваемых на основе принципа открытого распределения ключей.

3.4. Ключевые носители

Формирование закрытых ключей может производиться на следующие ключевые носители:

- дискета 3,5";
- процессорные карты MPCOS-EMV и российские интеллектуальные карты (РИК1, Оскар) с использованием считывателей смарт-карт, поддерживающий протокол PS/SC (GemPlus GCR-410, Towitoko, Oberthur OCR126);
- таблетки Touch-Memory DS1995 – DS1996 с использованием устройств Аккорд-АМДЗ, электронный замок "Соболь" или устройство чтения таблеток Touch-Memory DALLAS (DS9097E, DS9097U, DS1410E);
- электронный ключ с интерфейсом USB (e-Token);
- сменный носитель с интерфейсом USB;
- реестр Windows для варианта исполнения 1.
- Раздел /var/CPROcsp/users/ жёсткого диска для вариантов исполнения 2, 3, 4, 5.



Примечания. 1. Допускается хранение закрытых ключей в реестре ОС Windows для варианта исполнения 6 и в разделе HDD для вариантов исполнения 7, 8, 9, 10 при условии распространения на HDD ПЭВМ или ПЭВМ требований по обращению с ключевыми носителями.

2. Перечень ключевых носителей уточняется по исполнениям СКЗИ (см. Формуляр ЖТЯИ.00015-01 30 01).

3. Перечень ключевых носителей может расширяться.

3.5. Размеры ключей

Размеры ключей электронной цифровой подписи:

закрытый ключ – 256 бит;

открытый ключ – 1024 бита на базе алгоритма ГОСТ Р 34.10-94
- 512 бит на базе алгоритма ГОСТ Р 34.10-2001

Размеры ключей, используемых при шифровании:

закрытый ключ – 256 бит;

открытый ключ – 1024 бита на базе алгоритма ГОСТ Р 34.10-94
- 512 бит на базе алгоритма ГОСТ Р 34.10-2001

симметричный ключ – 256 бит;

4. Архитектура ПО и общие принципы функционирования

Основной архитектурной особенностью ПО СКЗИ КриптоПро CSP является то, что ПКЗИ не имеет непосредственного доступа к ключевой и криптографически значимой информации. Все операции с закрытыми и сессионными (симметричными) ключами, незавершенными значениями хэш-функций и т. п. осуществляется через дескрипторы соответствующих объектов; дескриптор объекта непосредственно не содержит его адреса. В качестве дополнительной меры защиты реализован

Криптографический сервис для хранения объектов в отдельном от ПКЗИ адресном пространстве.

4.1. Состав программного обеспечения

В состав программного обеспечения для всех платформ входят СКЗИ КриптоПро CSP, модуль сетевой аутентификации КриптоПро TLS и ПКЗИ.

Конкретизация состава СКЗИ, модуля сетевой аутентификации и ПКЗИ приводится для каждой платформы в соответствующем дополнении к данному документу.

Общая структура СКЗИ КриптоПро CSP версии 3.0 представлена на рис. 3.

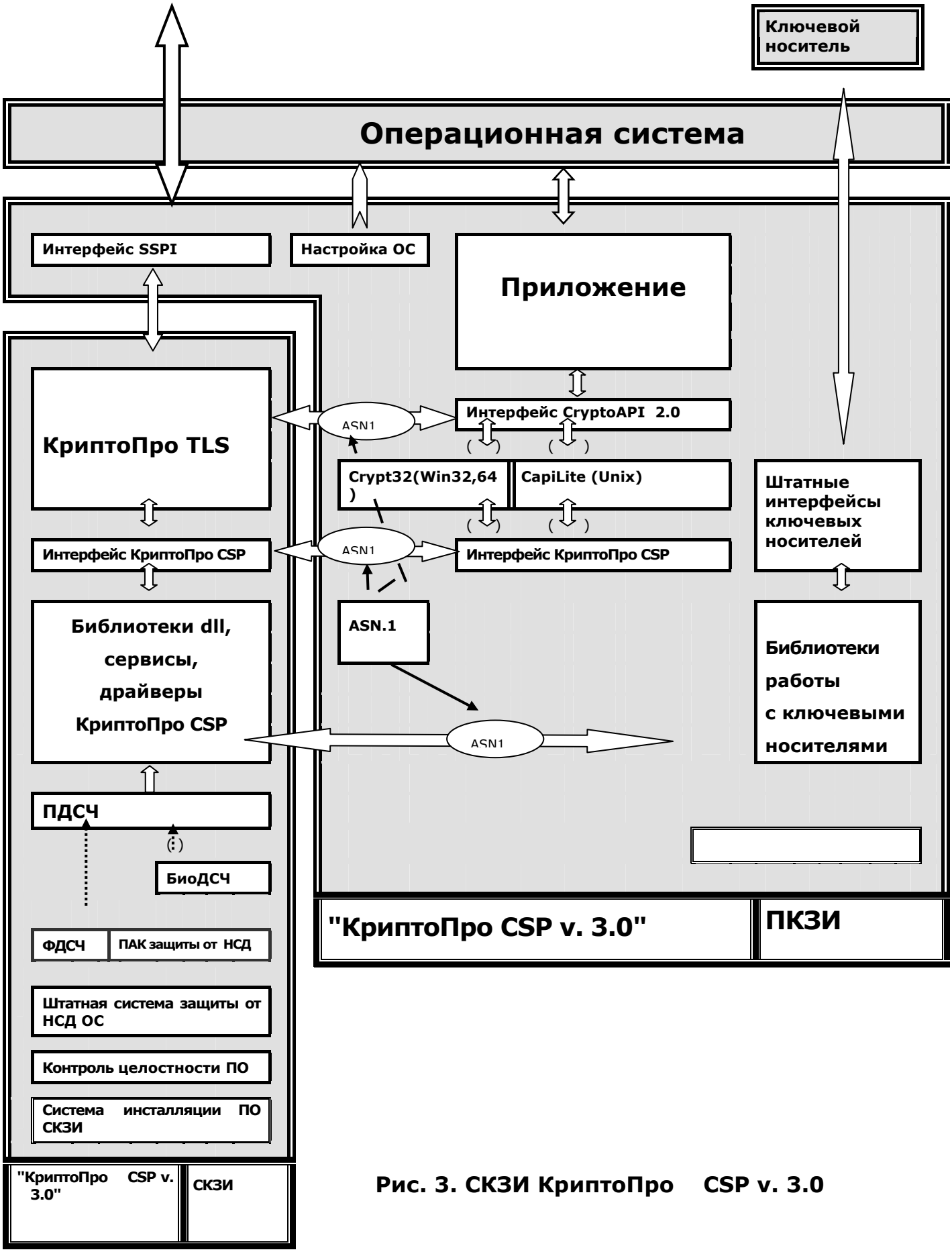


Рис. 3. СКЗИ КриптоПро CSP v. 3.0

4.2. СКЗИ КриптоПро CSP

В состав СКЗИ КриптоПро CSP входят:

- Библиотеки криптопровайдера (динамические) для исполнений по уровню КС1;
- Сервис хранения ключей для исполнений по уровню КС2;
- Криптодрайвер;
- Библиотеки протокола сетевой аутентификации КриптоПро TLS;
- Программно-аппаратный комплекс защиты от НСД (типа "Соболь", "Аккорд-АМДЗ") для всех исполнений уровня **КС2**, исключая платформы Solaris 9 Update 4 (SPARC);
- Подсистема контроля целостности в форме библиотеки либо драйвера в зависимости от исполнения СКЗИ.

4.3. ПКЗИ КриптоПро CSP

В состав ПКЗИ входят следующие компоненты:

- Библиотека управления сертификатами открытых ключей CapiLite для исполнений под ОС Red Hat Linux, FreeBSD, Solaris;
- Библиотеки настройки ОС Windows, обеспечивающие совместимость CryptoAPI v 2.0 с ПО СКЗИ;
- Библиотеки работы с ключевыми носителями;
- ASN.1 модуль;
- Система настройки для обеспечения функционирования СКЗИ для исполнений под ОС Windows.

Состав модулей СКЗИ и ПКЗИ конкретизируется в соответствующих дополнениях к данному документу.

5. Описание протокола сетевой аутентификации КриптоПро TLS

5.1. Назначение протокола TLS

Протокол TLS (Transport Layer Security, спецификация IETF - RFC2246) относится к средствам защиты прикладных пакетов Microsoft Internet Explorer, 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. Протокол SSL/TLS (SSL - более ранние версии протокола) применяется Интернет-протоколами (Таблица 1):

Таблица 1.

Протокол	Порт	Описание
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 SSLДLS
IRCS	994	IRC по SSL/TLS
IMAPS	993	IMAP (электронная почта) по SSL/TLS
FTPS	990	FTP (передача файлов) по SSL/TLS

Чтобы протокол SSL/TLS действовал, Web-сервер должен иметь сертификат (открытый ключ) и свой 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 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 делать).

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

5.2. Основные понятия протокола TLS

Протокол TLS предназначен для обеспечения криптографическими средствами аутентификации отправителя (клиента) – 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 организации информационного обмена

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.

Алгоритм преобразования информации при обмене

Алгоритм преобразования информации при обмене с использованием протокола TLS включает 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);
- хеширование фрагментов (используется ключевой MAC);

- конкатенация фрагмента и результата его хэширования (расширенный фрагмент);
- зашифрование расширенного фрагмента (опционально);
- передача зашифрованного расширенного фрагмента с добавленным открытым заголовком протокола транспортного уровня (например, TCP).

При приеме информации применяется обратная последовательность операций.

Атрибуты сессии

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.

Атрибуты соединения

К атрибутам соединения относятся:

- client_random – случайные 32 байта, задаваемые клиентом;
- server_random– случайные 32 байта, задаваемые сервером;
- client write MAC secret (ключ клиента для ключевого хэширования);
- server write MAC secret (ключ сервера для ключевого хэширования);
- 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: $0 \div 2^{64}-1$.

Соединение ассоциируется с одной сессией.

Типы сообщений

В протоколе TLS используются следующие типы сообщений:

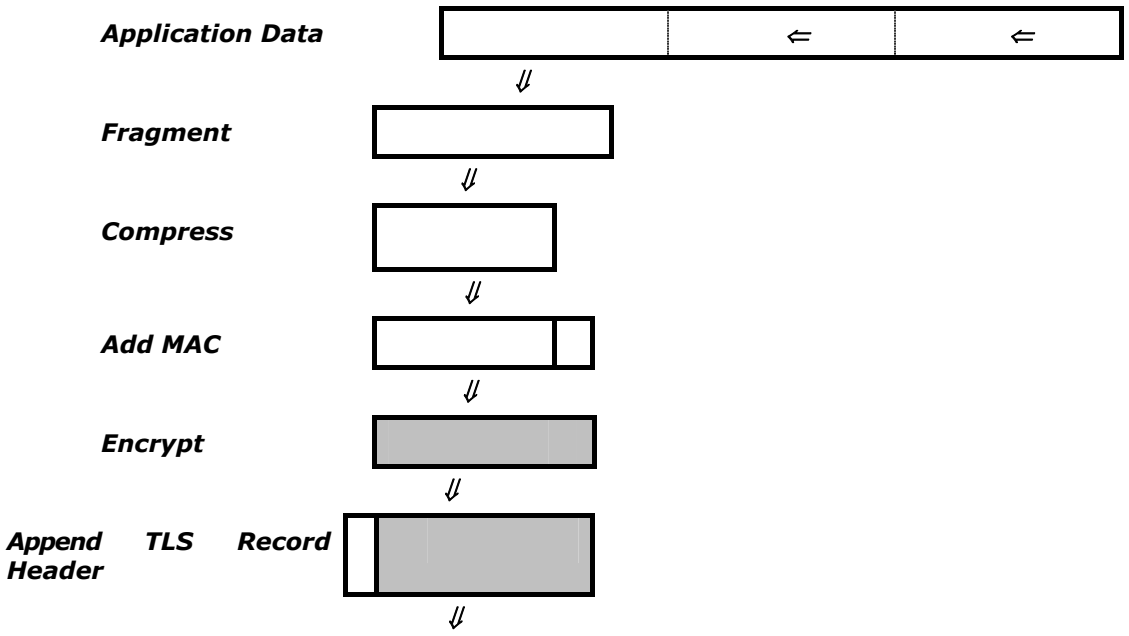
- Hello message (ClientHello, ServerHello);
- Change cipher specs message (изменение спецификации алгоритмов и параметров защиты);
- Key exchange message (передача ключа обмена ключами шифрования и MAC клиента, сервера);
- Alert message (предупреждение, оповещение о фатальной ошибке);
- Application_data message (передача данных);
- Finished message (сообщение о возможности работы в созданной сессии).

Фрагмент сообщения, передаваемый протоколу транспортного уровня

Для передачи фрагмента сообщения транспортному уровню производятся операции:

- компрессия фрагмента (опционально);
- вычисление хэша от конкатенации ключа хэширования, типа компрессии, длины компрессированного фрагмента, компрессированного фрагмента, заданной константы;
- шифрование расширенного фрагмента (конкатенация компрессированного фрагмента и его хэша);
- добавление открытого заголовка, содержащего тип сообщения (один байт), версию протокола TLS (два байта), длину компрессированного фрагмента.

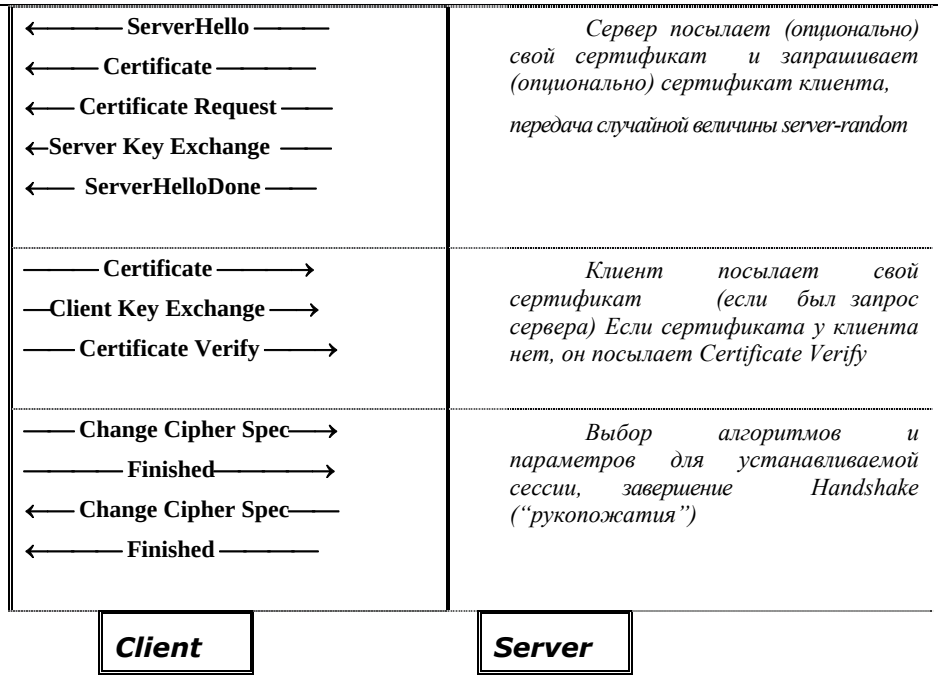
Операции протокола TLS



TLS Handshake Protocol

TLS Handshake Protocol работает по следующей схеме:

ClientHello →	*Установка версии протокола, идентификатора сессии, начального набора алгоритмов и параметров, метода компрессии*

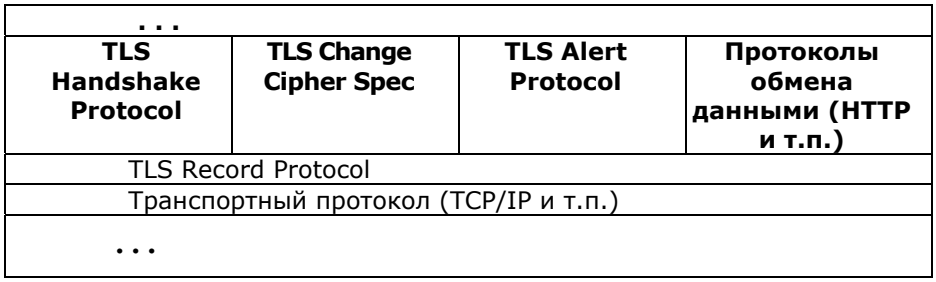


TLS Handshake Protocol обеспечивает инициализацию сессии (соединения) выполнением операций:

- 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.

Стек протокола TLS

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



5.3. Модуль поддержки сетевой аутентификации КриптоПро TLS

Модуль поддержки 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 цифровой подписи в соответствии с ГОСТ Р 34.10-94 или ГОСТ Р 34.10-2001. , хэширования в соответствии с ГОСТ Р 34.11-94). Используется также алгоритм Диффи-Хеллмана открытого распределения ключей на базе ГОСТ Р 34.10-94 или ГОСТ Р 34.10-2001.

На ПЭВМ клиента и на сервере (IIS, ISA) устанавливается СКЗИ "КриптоПро CSP" v. 3.0 с модулем поддержки сетевой аутентификации КриптоПро TLS.

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 сертификата, однако при этом он лишается возможности формировать электронную цифровую 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.

В СКЗИ «КриптоПро CSP» используется двусторонняя аутентификация.

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 цифровой подписи под электронными HTML-формами, заполняемыми пользователями.

Двусторонний метод аутентификации 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 Удостоверяющем центре.

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.

Требования к сертификату:

- 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 осуществляется через АРМ пользователя Центра регистрации. Порядок действий определяется в инструкции пользователю.

6. Ключевая система и ключевые носители

6.1. Общие положения

СКЗИ КриптоПро CSP является системой с открытым распределением ключей. Открытые ключи подписи и шифрования обычно представляются в виде сертификатов открытых ключей.

В СКЗИ КриптоПро CSP закрытый ключ подписи может быть использован только для формирования ЭЦП. Закрытый ключ шифрования может быть использован как для формирования ключа связи с другим пользователем, так и для формирования ЭЦП.

При работе с СКЗИ каждый пользователь, обладающий правом подписи и/или шифрования, вырабатывает на своем рабочем месте или получает у администратора безопасности (в зависимости от принятой политики безопасности) личные закрытый и открытый ключи. На основе каждого открытого ключа третьей стороной (Центром Сертификации) формируется сертификат открытого ключа.

Должны быть приняты меры, обеспечивающие сохранение в тайне закрытых ключей электронной подписи и шифрования и соответствующий порядок работы с ключевой документацией и сертификатами открытых ключей.

6.1.1. Шифрование данных

В СКЗИ КриптоПро CSP ключ зашифрования сообщения совпадает с ключом расшифрования (общий закрытый ключ связи). При зашифровании сообщения пользователя А для пользователя Б общий закрытый ключ связи вырабатывается на основе закрытого ключа шифрования пользователя А и открытого ключа шифрования пользователя Б. Соответственно, для расшифрования этого сообщения пользователем Б формируется общий закрытый ключ связи на основе своего собственного закрытого ключа шифрования и открытого ключа шифрования пользователя А.

Таким образом, для обеспечения связи с другими абонентами каждому абоненту необходимо иметь:

- собственный закрытый ключ шифрования;
- открытые ключи шифрования (сертификаты открытых ключей) других пользователей.

6.1.2. Формирование и проверка ЭЦП

Закрытый ключ подписи используется для выработки электронной цифровой подписи. При проверке подписи проверяющий должен располагать открытым ключом (сертификатом) пользователя, поставившего подпись. Проверяющий должен быть полностью уверен в подлинности открытого ключа, а именно в том, что имеющийся у него открытый ключ соответствует открытому ключу конкретного пользователя. Для этой цели используется сертификат открытого ключа, подписанный третьей доверенной стороной. Каждому пользователю, обладающему правом подписи, необходимо иметь:

- закрытый ключ подписи;
- открытые ключи подписи (сертификаты открытых ключей) других пользователей.

6.2. Ключевой контейнер

При формировании закрытые ключи СКЗИ КриптоПро CSP записываются на ключевой носитель (ключевой контейнер).

Ключевой контейнер может содержать:

- только ключ подписи;
- только ключ шифрования;
- ключ подписи и ключ шифрования одновременно.

Единственный ключ ключевого контейнера либо ключ подписи в дальнейшем называется главным ключом, а ключ шифрования, в случае хранения в контейнере двух ключей, - вторичным ключом.

Дополнительно ключевой контейнер содержит 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.

6.3. Структура ключевого контейнера

Ключевой контейнер содержит следующую информацию:

главный ключ, маски главного ключа, контрольную информацию главного 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.

Структура ключевого контейнера обеспечивает чтение ключей и соответствующих масок отдельными операциями в раздельные области памяти, для чего он разбит на шесть зон (реализация зон зависит от типа ключевого носителя).

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

6.4. Формирование ключей

Формирование ключей пользователя производится с использованием функции **CPGenKey** (см. ЖТЯИ.00015-01 90 04) и спецификацией типа формируемого ключа: AT_KEYEXCHANGE или AT_SIGNATURE.

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**.



Примечания.

1. Закрытые ключи ЭЦП и шифрования формируются с использованием программного и физического (клавиатура-мышь) ДСЧ для исполнений 1-5, обеспечивающих защиту по уровню КС1; с использованием программного и физического ДСЧ ПАК «Аккорд» или «Соболь» для исполнений 6, 7 и 8, обеспечивающих защиту по уровню КС2. Для исполнений 9 и 10 генерация пользовательских ключей должна быть исключена; ключи для этих исполнений могут быть получены на рабочих местах, оснащенных СКЗИ в исполнениях 6, 7 и 8.

2. При использовании считывателей смарт-карт или устройств чтения таблеток Touch-Memory DALLAS необходимо проверить настройки COM портов ПЭВМ в BIOS и ОС. При отключенных COM портах (disabled) работа со считывателями будет невозможна.

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.

6.5. Хранение ключевых носителей

Личные ключевые носители пользователей рекомендуется хранить в сейфе. Пользователь несет персональную ответственность за хранение личных ключевых носителей.

При наличии в организации, эксплуатирующей СКЗИ, администратора безопасности, и централизованном хранении ключевых носителей, администратор безопасности организации несет персональную ответственность за хранение личных ключевых носителей пользователей. Личные ключевые носители администратора безопасности должны храниться в его личном сейфе.

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

Настоятельно рекомендуется использовать парольную защиту при хранении ключей в реестре ПЭВМ.

СКЗИ КриптоПро CSP может функционировать и хранить ключевую информацию в двух режимах:

- в памяти приложения для исполнений 1-5.
- в "Службе хранения ключей", которая реализована в виде системного сервиса для исполнений 6-10.

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

6.6. Сроки действия ключей

При использовании ключей обязательным является выполнение условий:
- максимальный срок действия закрытых ключей шифрования и ЭЦП - 1 год 3 месяца;
- максимальный срок действия открытых ключей шифрования – 1 год 3 месяца;
- максимальный срок действия открытых ключей ЭЦП при использовании алгоритма ГОСТ Р 34.10-94 - 6 лет.
- максимальный срок действия открытых ключей ЭЦП при использовании алгоритма ГОСТ Р 34.10-2001 - 30 лет.

6.7. 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).

6.8. Интерфейс управления ключами СКЗИ

Последовательность действий при генерации закрытых ключей пользователей, управлении их паролями, управлении ключами при распределении секрета определена в документе «ЖТЯИ.00015-01 90 02-05. КриптоПро CSP. Инструкции по использованию КриптоПро CSP и TLS.»

7. Рекомендации по встраиванию и использованию ПО СКЗИ

Для обеспечения защиты электронных документов и создания защищенной автоматизированной системы в первую очередь используют 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.

Использование криптографических средств требует, как правило, применения также организационно-технических мер защиты.

При создании защищенной автоматизированной системы необходимо определить модель угроз и политику ее безопасности. В зависимости от политики безопасности определяется необходимый набор криптографических функций и организационно-технических мер, реализуемых в создаваемой системе.

СКЗИ КриптоПро CSP в первую очередь предназначено для встраивания в прикладное программное обеспечение. Функции СКЗИ КриптоПро CSP, 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 8, 9, FreeBSD 5, Solaris 9 Update 4) через интерфейс библиотеки capilite.dll, являющейся подмножеством интерфейса **CryptoAPI 2.0.** Для этих целей **в комплект поставки включается документ** ЖТЯИ.00015-01 90 04 "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.00015-01 90 04 "КриптоПро CSP. Руководство программиста", описывающий состав функций и тестовое ПО.
3. в стандартном прикладном ПО Microsoft.

Ниже приведен основной перечень требований, реализуемых при помощи криптографических методов.

7.1. Конфиденциальность информации

При передаче данных в сети обеспечивается использованием функций шифрования.

Для обеспечения НСД к информации при хранении (на дисках, в базе данных) допускается использование шифрования на производном (например, от пароля) ключе.

7.2. Идентификация и авторство

При сетевом взаимодействии (установлении сеанса связи) обеспечивается функциями ЭЦП при использовании их в процессе аутентификации (например, в соответствии с рекомендациями X.509 [X.509]). Одновременно при аутентификации должна использоваться защита от переповторов. Для этих целей может использоваться функция имитозащиты с вычислением имитовставки на сессионном ключе (симметричный ключ шифрования).

При электронном документообороте обеспечивается использованием функций ЭЦП электронного документа. Дополнительно должна быть предусмотрена защита от навязывания, переповтора электронного документа и целостность справочников открытых ключей ЭЦП.

7.3. Целостность

Обеспечивается использованием функций ЭЦП электронного документа. При использовании функций шифрования (без использования ЭЦП) обеспечивается имитозащитой. Для обеспечения целостности хранимых данных может быть использована функция хеширования или имитозащиты, но при этом не обеспечивается авторство информации.

7.4. Неотказуемость от передачи электронного документа

Обеспечивается использованием функций ЭЦП (подпись документа отправителем) и хранением документа с ЭЦП в течение установленного срока приемной стороной.

7.5. Неотказуемость от приема электронного документа

Обеспечивается использованием функций ЭЦП и квитированием приема документа (подпись квитанции получателем), хранением документа и квитанции с ЭЦП в течение установленного срока отправляющей стороной.

7.6. Защита от переповторов

Обеспечивается использованием криптографических функций ЭЦП, шифрования или имитозащиты с добавлением уникального идентификатора сетевой сессии (электронного документа) с последующей их проверкой приемной стороной или разработкой специализированного протокола аутентификации (обмена электронными документами).

7.7. Защита от навязывания информации

Защита от нарушителя с целью навязывания им приемной стороне собственной информации, переданной якобы от лица санкционированного пользователя (нарушение авторства информации). Обеспечивается использованием функций ЭЦП с проверкой атрибутов электронного документа и открытого ключа отправителя. В случае навязывания информации про компрометации ключа обеспечивается организационно-техническими мероприятиями. Например, созданием системы централизованного управления ключевой информацией (оповещением абонентов) или специализированных протоколов электронного документооборота.

7.8. Защита от закладок, вирусов, модификации системного и прикладного ПО

Обеспечивается совместным использованием криптографических средств и организационных мероприятий (см. 13).

7.9. Правила встраивания и использования СКЗИ КриптоПро CSP

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

1. При использовании открытых ключей должна быть обеспечена целостность и идентичность открытого ключа. Это может быть реализовано:
   - путем заверения открытого ключа ЭЦП доверенной стороной (например, в случае использования сертификатов открытых ключей);
   - путем доверенного распространения и хранения открытых ключей в виде справочников.
2. При использовании сертификатов открытых ключей, заверенных подписью доверенной стороны, должна быть обеспечена безопасная доставка и хранение сертификата открытого ключа доверенной стороны, с использованием которого проверяются остальные сертификаты открытых ключей пользователей.
3. Криптографическое средство, с помощью которого производится заверение открытых ключей или справочников открытых ключей, должно быть сертифицировано по классу, соответствующему принятой политике безопасности.

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

5. При вызове функций СКЗИ КриптоПро CSP в прикладном программном обеспечении необходимо проверять код завершения функции.

Например:

```
unsigned long           ErrorCode;
unsigned long           CPLastError;
HCRYPTPROV              hProv = 0;
. . .
ErrorCode = 0;
ErrorCode = CPFunction (hProv ...);
if (ErrorCode == 0) {
     CPGetProParam (hProv, PP_LAST_ERROR,
        (char*) &CPLastError,
        sizeof(unsigned long),
        0);
        if (CPLastError == GPE_CHECKPROC_TESTFAIL) {
            Критическая ошибка
           Аварийное завершение программы
        }
        Обработка некритических ошибок
}
```

8. Управление ключами СКЗИ

Управление ключами СКЗИ базируется на архитектуре PKI рекомендаций X 509 в части управления сертификатами открытых ключей и должна обеспечиваться Удостоверяющим центром (УЦ). В качестве УЦ может выступать Удостоверяющий центр КриптоПро УЦ [ЖТЯИ.00009-01 30 01. Удостоверяющий центр "КриптоПро УЦ". Формуляр.], но допускается использование Центра Сертификации корпорации Microsoft (Microsoft Certification Authority), или другие реализации, обеспечивающие выполнение целевых функций.

Рекомендации по управлению ключами приведены для КриптоПро УЦ, основанной на использовании сертификатов открытых ключей и исходя из наличия определенной организационной структуры управления ключами, элементами которой являются:

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

Краткое описание Удостоверяющего центра КриптоПро УЦ приведено в приложении (см. Приложение 4).



Примечание.

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

2. При использовании СКЗИ КриптоПро CSP в составе программного комплекса "КриптоПро УЦ" следует руководствовать документом ЖТЯИ.00015-01 90 04. КриптоПро CSP. Руководство программиста.

ЖТЯИ.00009-01 30 01. Удостоверяющий центр "КриптоПро УЦ". Формуляр].

Сертификат открытого ключа подписи или шифрования представляет собой структурированную двоичную запись в формате ASN.1, содержащую:

- имя субъекта или объекта системы, однозначно идентифицирующее его в системе;
- открытый ключ субъекта или объекта системы;
- дополнительные атрибуты, определяемые требованиями использования сертификата в системе;
- ЭЦП 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 рекомендации по управлению ключевой системой на всех этапах ее жизненного цикла, начиная с формирования ключей Центра Сертификации. Рекомендации 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.

8.1. Удостоверяющий центр

Удостоверяющий центр является структурным подразделением, обеспечивающим 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 пользователей на основе полученных запросов и зарегистрированной информации;
- доставка сертификатов открытых ключей 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 цифровой подписью.

В состав программно-аппаратных средств 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.

8.2. 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. 8.11 "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 и 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).



Примечание. 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. [PKIX], [X.509]).

8.2.1. Закрытый ключ и сертификат ЦС

При формировании закрытого ключа ЭЦП и сертификата ЦС рекомендуется использовать следующие значения.

Сроки действия:

- срок действия закрытого ключа ЦС, предназначенный для формирования ЭЦП сертификатов открытых ключей – до 5 лет;
- срок действия сертификата ЦС – не больше 10 лет.

8.3. 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.

8.4. Формирование ключей Центра Регистрации

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

8.4.1. Регистрация Центра Регистрации

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

8.4.2. Ключ и сертификат ЦР

При формировании закрытого ключа и сертификата ЦР следует использовать следующие значения.

Сроки действия:

- срок действия закрытого ключа ЦР – 1 год 3 месяца;
- срок действия сертификата ЦР – не больше 6 лет.

8.4.3. 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.

8.5. Формирование ключей пользователя

Общая схема, используемая для включения пользователя в систему, состоит из следующих этапов:

1. регистрация пользователя;
2. формирование пользователем личных ключей (запроса на сертификат);
3. передача запроса в Центр Регистрации;
4. верификация запроса Центром Регистрации;
5. формирование сертификата пользователя;
6. получение сертификата пользователям.

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).

Формирование ключей пользователя происходит в следующей последовательности.

8.5.1. Регистрация пользователя

1. Пользователя системы или администратор безопасности, прибывают в Удостоверяющий Центр (Центр Регистрации) с документами, необходимыми для регистрации пользователя в системе.
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 (см. Рис. 4. Карточка оповещения о компрометации).

   В **Карточке оповещения** указаны: телефоны УЦ, пароль (кодовое слово) администратора УЦ, уникальный пароль (кодовое слово), присвоенный пользователю УЦ.



Примечание. Карточка оповещения используется участниками системы для сообщений о компрометации ключа по телефонным каналам общего пользования. **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

Рис. 4. 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".



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

8.5.2. Ключ и сертификат пользователя

При формировании закрытого ключа и сертификата пользователя следует использовать следующие значения.

Сроки действия:

- срок действия закрытого ключа пользователя– до 1 года 3 месяцев;
- срок действия сертификата пользователя – не больше 6 лет.

8.5.3. 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. Рекомендуется обеспечить защищенную доставку и хранение сертификата ЦС на ПЭВМ пользователя.
2. Пользователь производит формирование личного закрытого ключа и запроса на сертификат, содержащего открытый ключ 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".

8.5.4. 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 так же передается заверенный администратором бланк запроса и сертификата пользователя. Вторые копии этих бланков хранятся в ЦС (ЦР).

8.6. Повторная регистрация пользователя

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

8.7. Плановая смена ключей

8.7.1. Смена ключей Центра Сертификации

Заблаговременно (до окончания срока действия закрытого ключа ЦС) администратор ЦС производит формирование нового закрытого ключа и сертификата ЦС (см. 8.2 "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 во время, оставшееся до окончания срока действия закрытого ключа ЦС, обязаны получить новый сертификат ЦС и добавить его в справочники сертификатов, без удаления действующего сертификата ЦС.

8.7.2. 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. 8.7.3 "Смена ключей пользователя").

Все пользователи системы во время, оставшееся до окончания срока действия закрытого ключа ЦР, обязаны получить новый сертификат ЦР.

8.7.3. Смена ключей пользователя

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

Формирование нового закрытого ключа, запроса на сертификат, передача запроса в ЦР и получение сертификата производится согласно последовательности, описанной в разделе 8.5 " Формирование ключей ".

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

8.8. Компрометация ключей

Определение термина **Компрометация**, виды компрометации и основные события, приводящие к компрометации, приведены в разделе Основные термины и положения.

По факту компрометации ключей должно быть проведено служебное расследование.

Выведенные из действия скомпрометированные ключевые носители после проведения служебного расследования уничтожаются, о чем делается запись в "Журнале пользователя сети".

8.8.1. 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.

8.8.2. 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, для восстановления системы необходимо:

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

8.8.3. 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" (см. Рис. 4. Карточка 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 ЭЦП и передачи запроса в защищенном виде по сети, запрос на сертификат вместе с бланками доставляется лично пользователем (администратором безопасности) в Центр Регистрации.

8.8.4. 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 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. 8.5.1 "Регистрация пользователя"), может быть использована электронная почта.

Сертификат открытого ключа 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 ЭЦП.

8.9. 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 8.8.4 "Действия УЦ при компрометации ключей пользователя".

8.10. 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. 8.5.1 "Регистрация пользователя").

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

8.11. 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 ЭЦП, 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;



Примечание. Ориентировочные графы журналов приведены в приложениях (см. Приложение 2 и 3).

9. Порядок разбора конфликтных ситуаций, связанных с применением ЭЦП

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

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

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

Данный разбор основывается на математических свойствах алгоритма ЭЦП, реализованного в соответствии со стандартами Российской Федерации ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94, гарантирующем невозможность подделки значения ЭЦП любым лицом, не обладающим закрытым ключом подписи.

При проверке значения ЭЦП используется открытый ключ, значение которого вычисляется по значению закрытого ключа ЭЦП при их формировании.

В системе должны быть предусмотрены средства ведения архивов электронных документов с ЭЦП и сертификатов открытых ключей.

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 системы (Договору), заключаемому между участниками автоматизированной системы.

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

9.1. Порядок разбора конфликтной ситуации

Разбор конфликтной ситуации выполняется по инициативе любого участника автоматизированной системы 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 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 ЭЦП;
2. проверка ЭЦП электронного документа с использованием каждого сертификата;

3. определение даты формирования каждой ЭЦП в электронном документе;
4. проверка ЭЦП 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 ЭЦП;
7. проверка отсутствия сертификатов в СОС.

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



Примечание. Несовпадение даты формирования документа и сроков действия сертификата и/или сроков действия закрытого ключа **не влияют** на определение авторства документа. На их основе можно сделать предположение о несоблюдении пользователем Регламента (Договора) в части сроков действия ключей, сертификатов или некорректного использования сертификата в прикладном ПО.

9.2. Случаи невозможности проверки значения ЭЦП

При не обнаружении в архиве сертификата открытого ключа пользователя, выполнившего ЭЦП, 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.

10. Нештатные ситуации при эксплуатации СКЗИ

Ниже приведен основной перечень нештатных ситуаций и соответствующие действия персонала при их возникновении.

Таблица 2. Действия персонала в нештатных ситуациях

№ п/п	Нештатная ситуация	Действия персонала
	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 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.
	Компрометация одного из личных ключевых носителей.	Порядок действий при компрометации ключей описан в разделе 8.8.3 "Компрометация ключей пользователя".
	Выход из строя первого личного ключевого носителя. Аналогично для носителей Touch Memory и смарт-карт.	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.
	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).
	Отказы и сбои в работе аппаратной части АРМ со встроенной СКЗИ.	При отказах и сбоях в работе аппаратной части АРМ со встроенной СКЗИ необходимо остановить работу, по возможности локализовать неисправность и в дальнейшем произвести ремонт в установленном порядке и, при необходимости, переустановку СКЗИ.
	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.
	Утеря личного ключевого носителя.	Утеря личного ключевого носителя приводит к компрометации ключей. Порядок действий при компрометации ключей описан в разделе 8.8.3 "Компрометация ключей пользователя".
	Отказы и сбои в работе	При отказах и сбоях в работе программных средств, в следствии

№ п/п	Нештатная ситуация	Действия персонала
	программных средств вследствие не выявленных ранее ошибок в программном обеспечении.	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.
9.	Отказы в работе программных средств вследствие случайного или умышленного их повреждения.	При отказах в работе программных средств, в следствии 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, в следствии 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. 8.11 "Ведение журналов").

11. Рекомендации по размещению технических средств с СКЗИ

При размещении технических средств использующих СКЗИ, следует руководствоваться следующими рекомендациями:

1. Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях.
2. Входные двери режимных помещений должны быть оборудованы замками, гарантирующими надежное закрытие помещений в нерабочее время.
3. Окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией.
4. Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам, а также требованиям пожарной безопасности.
5. Внутренняя планировка и расположение рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений.
6. По окончании рабочего дня помещения закрываются и опечатываются. Помещения с опечатанными входными дверьми сдаются под охрану отделу безопасности или дежурному по предприятию (по установленному порядку) с указанием времени приема-сдачи с отметкой о включении и выключении охранной сигнализации в журнале учета.
7. Сдачу ключей и помещений под охрану, также получение ключей и вскрытие помещений производят сотрудники, работающие в этих помещениях, по утвержденному руководством учреждения списку с образцами подписей этих сотрудников, который находится у охраны или у дежурного по учреждению.
8. Перед вскрытием помещений должна быть проверена целостность оттисков печатей и исправность замков. При обнаружении нарушения целостности

оттисков печатей, повреждения замков или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, помещение не вскрывается, а о случившемся немедленно ставится в известность руководство и отдел безопасности.

9. В случае утраты ключа от входной двери помещения немедленно ставится в известность отдел безопасности учреждения.
10. На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководством учреждения, в которых предусматривается порядок вызова администрации, должностных лиц, вскрытие помещений, очередность и порядок спасения конфиденциальных документов и дальнейшего их хранения.
11. Рекомендуется не использовать в помещении, где размещены рабочие места с установленным СКЗИ, радиотелефоны и другую радиоаппаратуру.

12. Рекомендации по установке ПО СКЗИ на ПЭВМ

К эксплуатации программного обеспечения, имеющего в своем составе СКЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие эксплуатационную документацию на соответствующие программные средства.

Установка ПО СКЗИ КриптоПро CSP осуществляется в соответствии с дополнениями к данному документу в зависимости от платформ.

При установке программного обеспечения СКЗИ, следует:

1. На технических средствах, оснащенных СКЗИ, использовать только лицензионное программное обеспечение фирм-изготовителей. Установленное программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.
2. Аппаратуру, на которой устанавливается СКЗИ, проверить на отсутствие аппаратных закладок.
3. Перед установкой СКЗИ проверить программное обеспечение ПЭВМ на отсутствие вирусов и программных закладок. Также рекомендуется исключить из программного обеспечения средства разработки и отладки программ.
4. При использовании СКЗИ в соответствии с классом КС2 в ПЭВМ должен быть установлен ПАК "Аккорд-АМДЗ", электронный замок "Соболь" или другое средство защиты от НСД, указанное в формуляре.
   Рекомендуется установка средств защиты от НСД и при использовании СКЗИ в соответствии с классом КС1.
5. Предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленной СКЗИ (путем опечатывания системного блока и разъемов ПЭВМ и контроля печатей администратором безопасности).
6. После завершения процесса установки провести контроль установленного ПО, а также его окружения (см. Приложение 4).

13. Требования по защите от НСД

СКЗИ КриптоПро CSP в варианте исполнения по уровню КС1 при условии выполнения настоящих Правил обеспечивают защиту конфиденциальной информации от внешнего нарушителя, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки.

СКЗИ КриптоПро CSP в варианте исполнения по уровню КС2 со средствами защиты от НСД при условии выполнения настоящих Правил обеспечивают защиту конфиденциальной информации также от внутреннего нарушителя, не являющегося пользователем средств вычислительной техники, на которых

реализованы СКЗИ и ПКЗИ, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки.

13.1. Принципы защиты информации от НСД

Защита информации от НСД в автоматизированной системе обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер. В их числе:

- применение специальных программно-аппаратных средств защиты;
- организация системы контроля безопасности информации;
- физическая охрана ПЭВМ и ее средств;
- администрирование информационной безопасности;
- учет носителей информации;
- сигнализация о попытках нарушения защиты;
- периодическое тестирование технических и программных средств защиты;
- использование сертифицированных программных и технических и средств.

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 может быть либо периодическим, либо инициироваться по мере необходимости пользователем или контролирующими органами.

В организации, эксплуатирующей ПО СКЗИ КриптоПро CSP, должна быть выпущена инструкция по защите от НСД к системе, разработанная на базе настоящего документа, руководящих документов Государственной технической комиссии, действующих нормативных документов самой эксплуатирующей организации.

В организации - пользователе системы должно быть выделено специальное должностное лицо - администратор безопасности, функции которого должны заключаться в выполнении процедур установки ПО, настройки системного окружения, установки, настройки, обслуживания и обеспечения функционирования средств защиты.

Администратор безопасности должен иметь возможность доступа ко всей информации, обрабатываемой на рабочем месте.

Каждый исполнитель работ как пользователь сети конфиденциальной связи должен быть зарегистрирован у администратора службы безопасности

При осуществлении доступа в глобальные сети передачи данных непосредственно с рабочих мест, оснащенных СКЗИ КриптоПро CSP, должны быть приняты меры, исключающие возможность воздействия нарушителя на СКЗИ по каналам связи, выходящим за пределы контролируемой зоны.

13.2. Организационные меры защиты информации от НСД

При использовании СКЗИ «КриптоПро CSP» следует принять следующие организационные меры:

1. Право доступа к рабочим местам с установленным ПО СКЗИ «КриптоПро CSP» предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе СКЗИ «КриптоПро CSP».
2. Запретить осуществление несанкционированного администратором безопасности копирование ключевых носителей.

3. Запретить разглашение содержимого ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер.
4. Запретить использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ «КриптоПро CSP», либо использовать ключевые носители на посторонних ПЭВМ.
5. Запретить запись на ключевые носители посторонней информации.
6. На технических средствах, оснащенных СКЗИ «КриптоПро CSP», должно использоваться только лицензионное программное обеспечение фирм-производителей.
7. На ПЭВМ, оснащенных СКЗИ «КриптоПро CSP», не допускается установка средств разработки и отладки ПО. Если средства отладки приложений необходимы для технологических потребностей пользователя, то их использование должно быть санкционировано администратором безопасности. В любом случае запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений, использующих СКЗИ «КриптоПро CSP». Необходимо исключить попадание в систему программ, позволяющих, пользуясь ошибками ОС, получать привилегии администратора.
8. Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства СКЗИ «КриптоПро CSP», по роду своей деятельности не являющихся персоналом, допущенным к работе в указанных помещениях.
9. Должно быть запрещено оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ «КриптоПро CSP» после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.
10. Администратором безопасности должно быть проведено опечатывание системного блока с установленным СКЗИ «КриптоПро CSP», исключающее возможность несанкционированного изменения аппаратной части рабочей станции.
11. Из состава системы должно быть исключено все оборудование, которое может создавать угрозу безопасности ОС. Также избегают использования любых нестандартных аппаратных средств, имеющих возможность влиять на нормальный ход работы компьютера или ОС.
12. При использовании СКЗИ «КриптоПро CSP» на ПЭВМ, подключенных к общедоступным сетям связи, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей.
13. В BIOS ПЭВМ определяются установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС.
14. Средствами BIOS должна быть исключена возможность отключения пользователями ISA и PCI устройств при использовании ПАК защиты от НСД, устанавливаемых в ISA и PCI разъем.
15. Вход в BIOS ПЭВМ должен быть защищен паролем, к которому предъявляются те же требования, что и к паролю администратора. Пароль для входа в BIOS должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС.
16. Средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты.
17. При загрузке ОС должен быть реализован контроль целостности программного обеспечения, входящего в состав СКЗИ «КриптоПро CSP», самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ.

18. Должно быть реализовано физическое затирание содержимого удаляемых файлов.

13.3. Средства защиты от НСД, применяемые в СКЗИ КриптоПро CSP

Средства защиты от НСД используются в исполнениях 6 -10 (на платформе IA32) СКЗИ КриптоПро CSP для достижения защищенности по уровню КС2.

13.3.1. Программно-аппаратный комплекс "Аккорд-АМДЗ"

Программно-аппаратный комплекс (ПАК) "Аккорд-АМДЗ" предназначен для защиты информации от НСД при ее обработке в ПЭВМ.

Аппаратная составляющая комплекса "Аккорд-АМДЗ" используется на следующих платформах:

- Windows 2000/XP/2003 (платформа IA32);
- Red Hat Linux 7, 9 (платформа IA32);
- FreeBSD 5 (платформа IA32);
- Solaris 9 Update 4 (платформа IA32).

ПАК "Аккорд-АМДЗ" обеспечивает:

- идентификацию, проверку подлинности, разграничение доступа к ресурсам ПЭВМ на уровне выполняемых задач и контроль доступа субъектов в систему (ПЭВМ);
- регистрацию и учет входа (выхода) пользователей в систему (из системы), запуска (завершения) программ и процессов, доступа пользователей к защищаемым файлам, изменения полномочий пользователей;
- обеспечение целостности программных средств.

В качестве идентификатора в ПАК "Аккорд-АМДЗ" используется персональный идентификатор DS 199x (таблетка Touch-Memory).

Установка и настройка ПАК "Аккорд-АМДЗ" на АРМ пользователя должна производиться в соответствии с эксплуатационной документацией на ПАК "Аккорд-АМДЗ". Перед эксплуатацией ПАК "Аккорд-АМДЗ" в составе АРМ пользователя необходимо ознакомиться с комплектом документации (в соответствии с ведомостью эксплуатационных документов – 11443195.4012-006 20-01) на данный комплекс и принять рекомендуемые в документации защитные организационные меры.



Примечание. Перед установкой ПАК "Аккорд-АМДЗ" ПЭВМ, используемые в качестве АРМ пользователей, должны быть проверены на предмет их корректного взаимодействия.

Установка программного обеспечения и аппаратной части комплекса "Аккорд-АМДЗ" на АРМ может выполняться специалистами поставщика СКЗИ или представителями службы информационной безопасности. Настройка комплекса "Аккорд-АМДЗ" 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.

13.3.2. 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.

Аналогично ПАК "Аккорд-АМДЗ", электронный замок "Соболь" используется на платформах

- Windows 2000/XP/2003 (платформа IA32);
- Red Hat Linux 7, 9 (платформа IA32);
- FreeBSD 5 (платформа IA32);
- Solaris 9 Update 4 (платформа IA32).

Система **Электронный замок** 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;
- контроль целостности физических секторов жесткого диска;
- 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.00300-04 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.

14. Обеспечение безопасности функционирования рабочих мест со встроенными средствами криптографической защиты

В данном разделе представлены основные рекомендации по организационно-техническим мерам защиты для обеспечения безопасности функционирования рабочих мест со встроенной СКЗИ.

1. Использование шифровальных средств для криптографической защиты информации подлежит лицензированию в соответствии с действующим законодательством РФ.
2. Рабочие места, на которые установлены СКЗИ, должны быть аттестованы комиссией. Результаты работы комиссии отражаются в "Акте готовности к работе" (см. Приложение 1).
3. Правом доступа к рабочим местам с установленным СКЗИ должны обладать только лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, использующего СКЗИ, с правилами пользования или с другими нормативными документами, созданными на их основе.
4. Должностные инструкции администратора безопасности (его заместителя) и ответственного исполнителя должны учитывать требования настоящих Правил.
5. При каждом включении рабочей станции с установленным СКЗИ необходимо проверять сохранность печатей системного блока и разъемов рабочей станции.
6. Администратор безопасности должен периодически (не реже 1 раза в 2 месяца) проводить контроль целостности и легальности установленных копий ПО на всех АРМ со встроенной СКЗИ с помощью программ контроля целостности.

7. В случае обнаружения "посторонних" (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией в составе представителей служб информационной безопасности организации - владельца сети и организации - абонента сети, где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения.
8. Не допускается оставлять без контроля вычислительные средства, входящие в состав СКЗИ, при включенном питании и загруженном программном обеспечении СКЗИ. При кратковременном перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана производится с использованием пароля доступа.
9. Пользователь должен запускать только те приложения, которые разрешены администратором безопасности.
10. Средствами BIOS должна быть исключена возможность отключения пользователями ISA-устройств.
11. ПО, установленное на ПЭВМ, не должно иметь встроенных средств разработки и отладки программ.
12. ПЭВМ, обеспечивающие удаленный вход пользователей из глобальной сети, (например RAS сервер) не должны использовать ПО СКЗИ.
13. Пароли, назначаемые пользователям, должны отвечать требованиям соответствующих инструкции и нормативных документов.

Не допускается:

1. Осуществлять несанкционированное копирование ключевых носителей.
2. Разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер (за исключением случаев, предусмотренных данными правилами).
3. Вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя.
4. Подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией.
5. Работать на компьютере, если во время его начальной загрузки не проходит встроенный тест ОЗУ, предусмотренный в ПЭВМ.
6. Вносить какие-либо изменения в программное обеспечение СКЗИ.
7. Изменять настройки, установленные программой установки СКЗИ или администратором.
8. Использовать синхропосылки, вырабатываемые не средствами СКЗИ.
9. Обрабатывать на ПЭВМ, оснащенной СКЗИ, информацию, содержащую государственную тайну.
10. Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ КриптоПро CSP.
11. Осуществлять несанкционированное вскрытие системных блоков ПЭВМ.
12. Приносить и использовать в помещении, где размещены средства СКЗИ, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер).

Литература

1. Закон РФ № 24-ФЗ от 20.02.95 г. "Об информации, информатизации и защите информации".
2. Закон РФ № 5485-1 от 21.07.93 г. "О государственной тайне".
3. Закон РФ № 2446-1 от 05.03.92 г. "О безопасности".
4. Закон РФ № 15-ФЗ от 16.02.95 г. "О связи".
5. Закон РФ № 5151-1 от 10.06.93 г. "О сертификации продукции и услуг".
6. Закон РФ № 5154-1, 1993 г. "О стандартизации".
7. Закон РФ № 4871-1, 1993 г. "Об обеспечении единства измерений".
8. Закон РФ № 4524-1 от 19.02.93 г. "О федеральных органах правительственной связи и информации".
9. Гражданский кодекс Российской Федерации. Ч. 1. Принят Государственной Думой 21 октября 1994 г. Одобрен Советом Федерации.
10. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
11. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
12. ГОСТ Р 34.10-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
13. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
14. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.
15. ГОСТ Р 50739-95. Государственный стандарт Российской Федерации. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
16. ГОСТ Р 1.0-92. Государственная система стандартизации Российской Федерации. Основные положения.
17. ГОСТ 16487-83. Делопроизводство и архивное дело. Термины и определения.
18. ГОСТ Р 50922-96. Государственный стандарт Российской Федерации. Защита информации. Основные термины и определения.
19. Положение о государственном лицензировании деятельности в области защиты информации. Утверждено Решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации № 10 от 27 апреля 1994 г.
20. Гостехкомиссия России. Руководящий документ. Защита от НСД к информации. Термины и определения. - М.: Воениздат, 1992.
21. Гостехкомиссия России. Концепция защиты информации в системах ее обработки, 1995.
22. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники (СВТ) и автоматизированных систем от НСД к информации. Москва, 1992 г.
23. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. Москва, 1992 г.
24. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. Москва, 1992 г.
25. Халянин Д.В., Ярочкин В.И. Основы защиты промышленной и коммерческой информации. Термины и определения: Словарь / ИПКИР. - М., 1994.

26. Бияшев Р.Г., Диев С.И., Размахнин М.К. Основные направления развития и совершенствования криптографического закрытия информации / Зарубежная радиоэлектроника. 1989. № 12. С. 76-91.

27. Толковый словарь по информатике. - М.: Финансы и статистика, 1991.

28. Терминология в области защиты информации: Справочник / ВНИИстандарт, 1993.

29. ЖТЯИ.00015-01 90 01. КриптоПро CSP. Формуляр.

30. ЖТЯИ.00015-01 90 01. КриптоПро CSP. Описание реализации.

31. ЖТЯИ.00015-01 90 02-01. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows 2000/XP/2003.

32. ЖТЯИ.00015-01 90 02-02. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС в ОС Red Hat Linux 7,9.

33. ЖТЯИ.00015-01 90 02-03. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС FreeBSD 5.

34. ЖТЯИ.00015-01 90 02-04. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Solaris 9 Update 4.

35. ЖТЯИ.00015-01 90 02-05. КриптоПро CSP. Инструкции по использованию КриптоПро CSP и TLS.

36. ЖТЯИ.00015-01 90 04. КриптоПро CSP. Руководство программиста.

37. ЖТЯИ.00009-01 30 01. Удостоверяющий центр "КриптоПро УЦ". Формуляр.

38. [X.680-X.699]. OSI NETWORKING AND SYSTEM ASPECTS. Abstract Syntax Notation One (ASN.1)

39. [X.509]. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.

40. [PKIX]. RFC 2459. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January 1999.

Приложение 1. Акт готовности к работе

УТВЕРЖДАЮ

_____
(должность)
_____
(наименование учреждения)
_____
(подпись) (Ф.И.О.)

АКТ

готовности к работе _____ с _____
(наименование учреждения) (наименование изделий)

"_____" _____ 199___г.

Комиссия в составе председателя _____ _____ и членов
(должность) (Ф.И.О.)

назначенная _____ составила настоящий акт о том, что помещение

эксплуатирующего органа _____, размещение _____, хранилища
название оборудование

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, объект_____ отвечает требованиям
название объекта

_____
_____
название инструкции

по обеспечению безопасности связи 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 2. 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	21.04.2000		Администратор безопасности
2		Иванов И. И.	Почтовый адрес: a.sidorov@acme.ru Должность:	01.05.2000		Оператор расчетной системы

Приложение 3. Журнал пользователя сети

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

Приложение 4. ПК «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 цифровой 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 многоролевой 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 открытого ключа 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 закрытых и открытых ключей ЭЦП и шифрования пользователя на рабочем месте пользователя;
    - Выполнение процедуры генерации личных закрытых и открытых ключей ЭЦП и шифрования на рабочем месте администратора Удостоверяющего Центра;
    - Выполнение процедуры генерации личных закрытых и открытых ключей ЭЦП уполномоченного лица Удостоверяющего Центра;

- Выполнение процедуры генерации личных закрытых и открытых ключей ЭЦП уполномоченного лица подчиненного Удостоверяющего Центра;

• Ведения реестра запросов и заявлений на сертификаты открытых ключей в электронном виде

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

• Ведение реестра сертификатов открытых ключей, изданных Удостоверяющим Центром в электронном виде

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

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

• Выполнение процедуры подтверждения подлинности ЭЦП

- Выполнение процедуры подтверждения подлинности ЭЦП в электронных документах;
- Выполнение процедуры подтверждения подлинности ЭЦП уполномоченного лица Удостоверяющего Центра в изданных сертификатах открытых ключей.

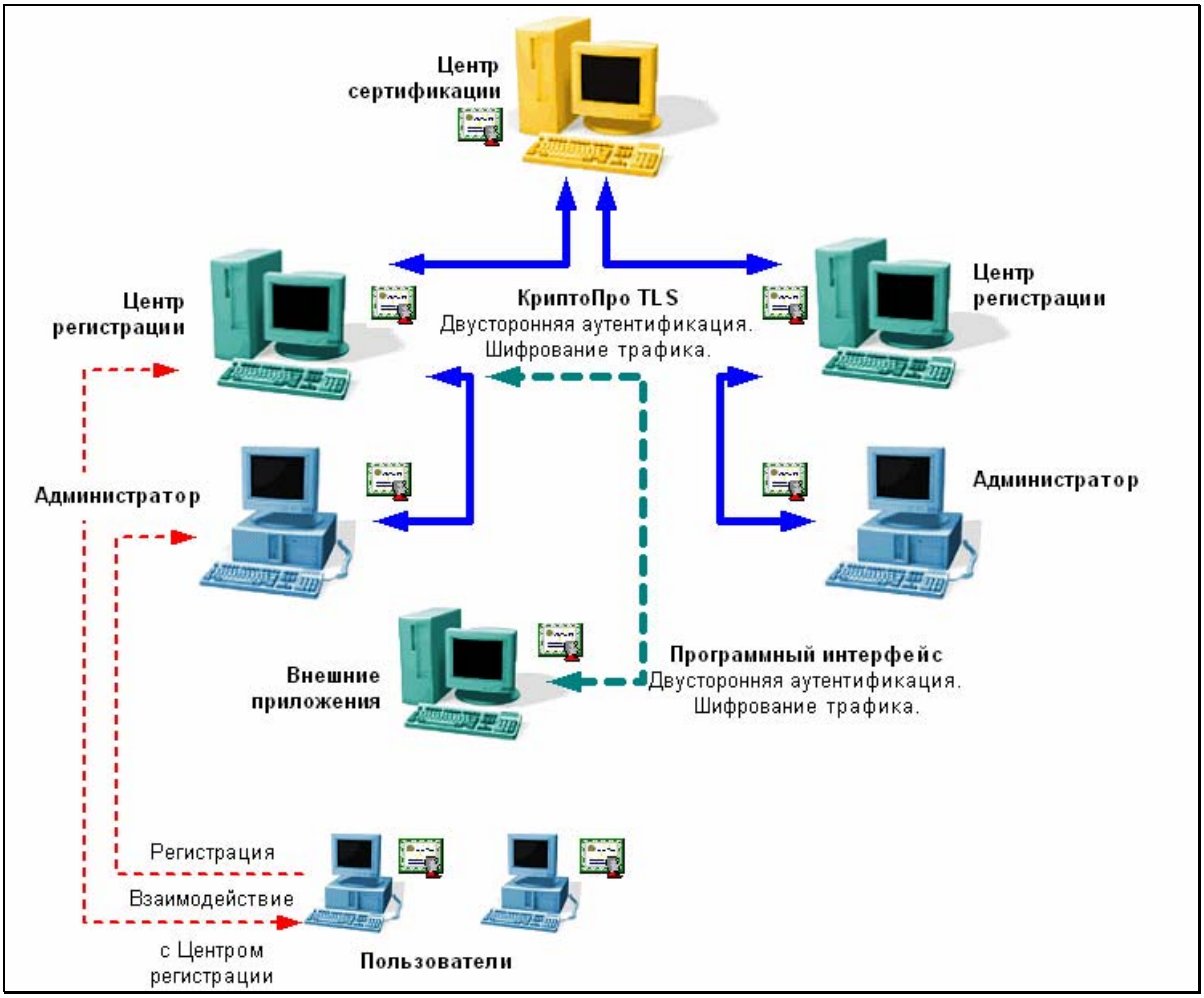
• Реализацию системы оповещения пользователей с использованием почтовых сообщений

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

Архитектура «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)



Центр Сертификации

Центр сертификации– компонент комплекса «КриптоПро УЦ», предназначенный для формирования сертификатов открытых ключей 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 2000 Server и использует базу данных SQL 2000 Server Desktop Edition.

SQL 2000 Server Desktop Edition устанавливается программой установки ПО Центра Сертификации.

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 ПАК «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 2000 Server и использует базу данных Microsoft SQL 2000 Server (Desktop Edition, Standard Edition или Enterprise Edition). Microsoft SQL 2000 Server Desktop Edition 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 2000 Professional или Windows 2000 Server. 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 ЭЦП в электронных документах и определения статуса сертификатов открытых ключей пользователей;
- с подтверждением подлинности ЭЦП уполномоченного лица Удостоверяющего Центра в изготовленных им сертификатах открытых ключей.

АРМ разбора конфликтных ситуаций функционирует в ОС Microsoft Windows 2000. 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 ЭЦП, 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 98 и выше (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 открытого ключа и получение служебного сертификата открытого ключа.

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 98 и выше (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 98 и выше (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»

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.

Управление 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.

Масштабируемость и производительность «КриптоПро УЦ»

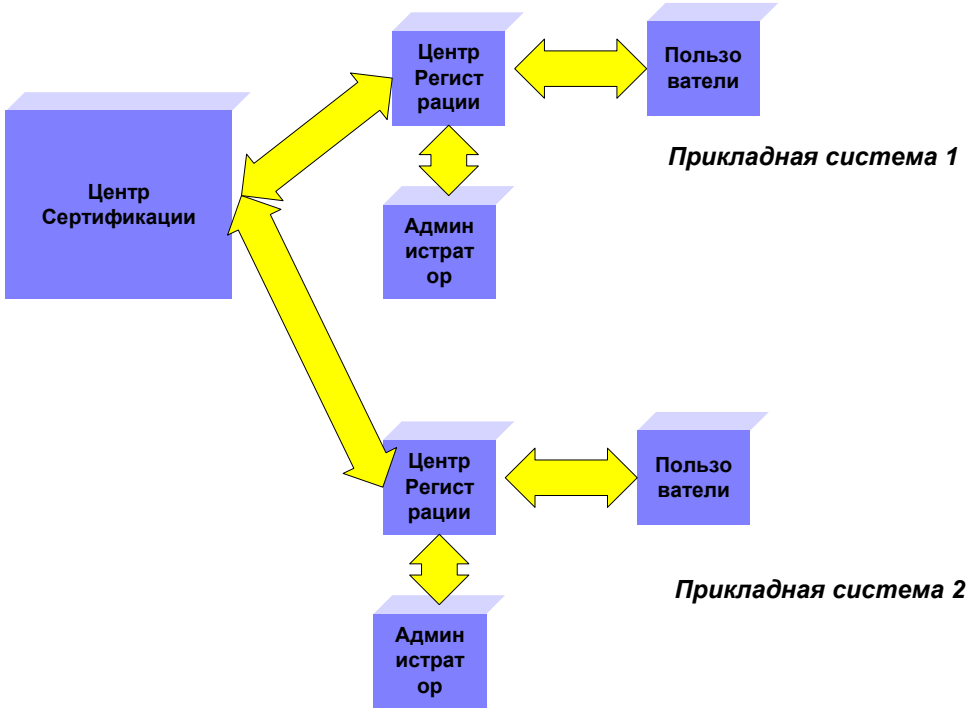
Масштабируемость

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.



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 выполняется нагрузочный тест по регистрации пользователей на «КриптоПро УЦ».

По состоянию на 12 января 2005 года зарегистрировано ***580 тысяч пользователей*** с генерацией ключей и изготовлением для каждого из них сертификата ключа подписи.

Индекс

А

Автоматизированная информационная система ... 8
Автоматизированная система ... 8
Авторство информации ... 8
Администратор защиты ... 8
Администратора безопасности ... 8
Актуальность информации ... 8
Аутентификация ... 8
Аутентификация информации ... 8

Б

Безопасность ... 9
Безопасность информации ... 9
Блокирование информации ... 9

В

Верификация ... 9
Владелец информации ... 9

Г

Государственная тайна ... 9
Гриф конфиденциальности ... 9
Гриф секретности ... 9

Д

Документ ... 10
Документ в электронной форме ... 10
Доступ к информации ... 10
Доступность информации ... 10

Ж

Журнал пользователя сети ... 46
Журнал регистрации администраторов безопасности и пользователей ... 46
Журналы ... 46

З

Защита информации ... 10
Защита информации от НСД ... 10
Защищенное средство вычислительной техники 11

И

Идентификация ... 11
Имитовставка ... 11
Имитозащита ... 11

К

Ключ ... 11
Компрометация ключа ... 11
Контроль доступа ... 12
Конфиденциальная информация ... 12
Конфиденциальность информации ... 12
Криптографический ключ ... 11
Криптографическое преобразование ... 13

Л

Лицензирование ... 13

М

Метка конфиденциальности ... 13

Н

Нарушитель безопасности информации 13
Нештатные ситуации 49
Носитель информации 14
НСД 13

О

Обработка информации 14
Объект доступа 14
Объект защиты 14
Открытый ключ 14

П

Пароль 14
Плановая смена ключей 14
Полномочный представитель организации 15
Пользователи 15
Правило доступа к защищаемой информации 15
Проверка электронной подписи документа 15

Р

Разбор конфликтов 46
Разглашение информации 15
Размещение технических средств 50
Расшифрование данных 15
Регламентация 15
Рекомендации по встраиванию 35

С

Секретный ключ 16
Сертификат защиты 16
Сертификат соответствия 16
Система защиты информации 16
Система защиты информации от НСД 16
Служебная и коммерческая тайна 16
Собственник информации 17
Способ защиты информации 17
Способы несанкционированного доступа 17
Средства вычислительной техники 18
Средство защиты информации 18
Средство защиты от несанкционированного доступа 18
Средство криптографической защиты информации 18
Субъект доступа 18

Т

Техническое средство обработки информации ... 18

У

Угроза безопасности 18
Уничтожение информации 18
Уничтожение ключевых документов 35
Управление ключами 18
Управление ключевой системой 37
Утечка информации 18

Ф

Функция хэширования 19

Х

Хранение ключевых документов 34

Ц

Целостность информации 19
Цель защиты информации 19

Ш

Шифр 19
Шифровальные средства 20
Шифрование 19

Э

Электронная цифровая подпись 20
ЭЦП 20

Лист регистрации изменений									
	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
Изм	измененных	замененных	новых	аннулированных					