127 018, Москва, Сущевский Вал, д.16/5
Телефон: (495) 780 4820
Факс: (495) 780 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство
Криптографической
Защиты
Информации

КриптоПро CSP

Версия 3.6

Руководство администратора безопасности

Общая часть

ЖТЯИ.00050-02 90 02
Листов 57

2010

Содержание

Аннотация

Настоящее Руководство содержит общее описание средства криптографической защиты информации КриптоПро CSP v. 3.6, ЖТЯИ.00050-02 (далее по тексту – СКЗИ ЖТЯИ.00050-02), рекомендации по использованию СКЗИ в различных автоматизированных системах.

В зависимости от комплектации и используемой программно-аппаратной среды функционирования СКЗИ следует руководствоваться также документами [9] - [17].

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
АРМ	Автоматизированное рабочее место
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск
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.
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.
СФК	Среда функционирования комплекса
ЦС	Центр Сертификации УЦ
УЦ	Удостоверяющий Центр
ЦР	Центр Регистрации УЦ
ЭД	Электронный документ
ЭЦП	Электронная цифровая подпись

2. Основные термины и понятия

Автоматизированная информационная система

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

Автоматизированная система

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

Авторство информации

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

Актуальность информации

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

Администратор безопасности

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

Основные направления деятельности администратора безопасности:

- контроль целостности программного обеспечения;

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

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

Администратор защиты

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

Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Аутентификация информации

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

Безопасность

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

Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба.

Безопасность информации (информационная безопасность)

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

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

Блокирование информации

Прекращение или затруднение доступа законных пользователей к информации.

Верификация

Установление соответствия принятой и переданной информации с помощью логических методов.

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

Владелец информации

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

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

Владелец информации, информационной системы

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

Государственная тайна

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

Гриф конфиденциальности

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

Гриф секретности

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

Документ

Документированная информация, снабженная определенными реквизитами.

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

Документированная информация (документ)

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

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

Документ в электронной форме (Электронный документ)

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

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

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

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

Доступность информации

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

Заверение (нотаризация)

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

Защита информации

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

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

Защита информации от НСД

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

Защищенное средство вычислительной техники (защищенная автоматизированная система)

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

IA32, IA64, x64, SPARC, Power PC

Аппаратные платформы, используемые производителями ПЭВМ

Идентификация

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

Имитозащита

Защита системы шифрованной связи от навязывания ложных данных.

Имитовставка

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

Ключ (криптографический ключ)

Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований [3].

Компрометация ключа

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

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

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

Конфиденциальность информации

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

Конфиденциальная информация

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

Контроль доступа (управление доступом)

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

Криптографическая защита

Защита данных при помощи криптографических преобразований данных.

Криптопровайдер

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

Криптопродрайвер

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

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

Криптосервис

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

Криптографическое преобразование

Преобразование информации с использованием криптографических алгоритмов.

Лицензирование в области защиты информации

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

Мероприятия по защите информации

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

Мероприятия по контролю эффективности защиты информации

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

Метка конфиденциальности

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

Нарушитель безопасности информации

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

Нарушитель правил разграничения доступа

Субъект доступа, осуществляющий несанкционированный доступ к информации.

Некорректный электронный документ

Электронный документ, не прошедший процедуры расшифрования данных, проверки электронной 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.

Несанкционированное воздействие на информацию

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

Несанкционированный доступ к информации (НСД)

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

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

Носитель информации

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

Объект доступа

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

Объект защиты

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

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

Обработка информации

Передача, прием, хранение, преобразование и отображение информации.

Организация защиты информации

Содержание и порядок действий по обеспечению защиты информации.

Открытый ключ

Криптографический ключ, который связан с закрытым с помощью особого математического соотношения. Открытый ключ известен всем другим пользователям системы и предназначен для проверки электронной 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.

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

Плановая смена ключей

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

Побочные электромагнитные излучения и наводки

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

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

Побочное электромагнитное излучение

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

Пользователи

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

Пользователь (потребитель) информации

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

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

Полномочный представитель организации

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

Правило доступа к защищаемой информации

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

Правила разграничения доступа (ПРД)

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

Право доступа к защищаемой информации; право

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

Проверка электронной подписи документа

Проверка соотношения, связывающего хэш-функцию документа, подпись под этим документом и 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.

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

Расшифрование данных

Процесс преобразования зашифрованных данных в открытые данные при помощи шифра.

Регламентация

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

Санкционированный доступ к информации

Доступ к информации, не нарушающий правила разграничения доступа.

Сертификат защиты

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

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

Сертификат соответствия

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

Секретный (закрытый) ключ

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

Система защиты информации от НСД

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

Служебная и коммерческая тайна

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

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

Собственник информации

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

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

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

Способ защиты информации

Порядок и правила применения определенных принципов и средств защиты информации.

Способы несанкционированного доступа

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

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

2. К основным способам НСД относятся:

- непосредственное обращение к объектам доступа;

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

3. модификация средств защиты, позволяющая осуществить НСД;

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

Средства вычислительной техники

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

Средство защиты информации

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

Средство защиты от несанкционированного доступа

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

Средство криптографической защиты информации

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

Субъект доступа

Лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Субъект информационных отношений

Физическое или юридическое лицо, обладающее определенным правом по отношению к информационному ресурсу. В зависимости от уровня полномочий субъект информационных отношений может быть источником, собственником, владельцем или пользователем информации.

Техническое средство обработки информации

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

Угроза безопасности

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

Удостоверяющий центр

Центр управления открытыми ключами 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.

Управление ключами

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

Утечка информации

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

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

Функция хэширования

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

Целостность информации

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

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

Цель защиты информации

Заранее намеченный результат защиты информации.

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

2. Целями защиты являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение угроз безопасности личности, общества, государства; предотвращение

несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах, сохранение государственной тайны конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Шифр

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

Шифрование

Процесс зашифрования или расшифрования.

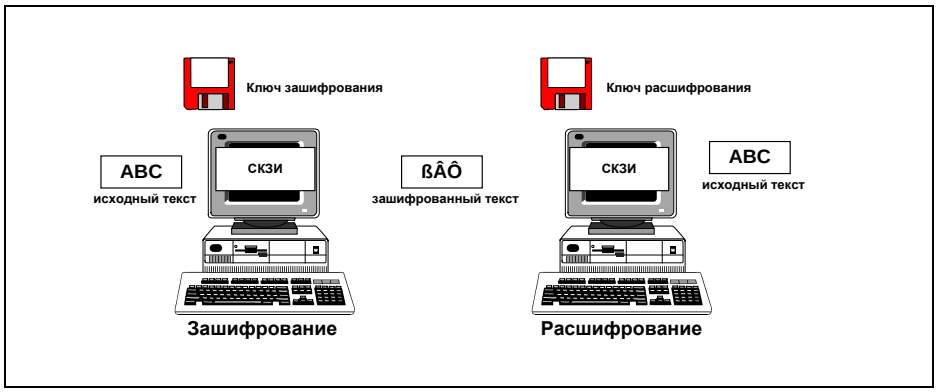


Рис. 1. Шифрование информации

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.

4. ручные шифры, документы кодирования и другие носители ключевой информации.

Шифрующая файловая система

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

Электронная 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. Назначение, основные технические данные и характеристики СКЗИ

3.1. Назначение СКЗИ. Условия эксплуатации

СКЗИ ЖТЯИ.00050-02 предназначено для защиты открытой информации в информационных системах общего пользования (вычисление/проверка электронной цифровой подписи) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах (шифрование/расшифрование информации, вычисление/проверка имитовставки, вычисление значения хэш-функции, вычисление/проверка электронной цифровой подписи).

Средствами СКЗИ ЖТЯИ.00050-02 **НЕ ДОПУСКАЕТСЯ** обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

СКЗИ ЖТЯИ.00050-02 **МОЖЕТ ИСПОЛЬЗОВАТЬСЯ** для криптографической защиты персональных данных.

3.2. Программно-аппаратные среды функционирования СКЗИ

СКЗИ ЖТЯИ.00050-02 является модификацией СКЗИ КриптоПро CSP версии 3.6 (СКЗИ ЖТЯИ.00050-01), совместимо с ним по выполняемым криптографическим функциям и отличается расширением и обновлением программно-аппаратных сред функционирования, предоставлением дополнительных криптографических услуг. СКЗИ ЖТЯИ.00050-02 выпускается в двух исполнениях, отличающихся программно-аппаратной средой функционирования, составом программных модулей и классом защиты (КС1, КС2).

СКЗИ ЖТЯИ.00050-02 функционирует в программно-аппаратных средах:

- Windows 2000 (ia32);
- Windows XP/2003/Vista/2008/7/2008R2 (ia32, ia64, x64).

- Linux Standard Base ISO/IEC 23360 (ia32, x64), программно-аппаратные среды, удовлетворяющие стандарту LSB 4.x/3.x:
  - Linpus (ia32)
  - Mandriva (ia32, x64)
  - MontaVista Linux (ia32, x64)
  - Oracle Enterprise Linux (ia32, x64)
  - Open SUSE (ia32, x64)
  - Red Hat Enterprise Linux (ia32, x64)
  - Red Flag Linux (ia32)
  - SUSE Linux Enterprise (ia32, x64)
  - SUSE LINUX (ia32)
  - Ubuntu (ia32, x64)
  - Xandros (ia32)

  ALT Linux (ia32, x64);
  Debian (ia32, x64);
  Red Hat Enterprise Linux Version 3 Update 3 (ia32, x64);
  Trustverse Linux XP (ia32);
- FreeBSD 7/8 (ia32);
- Solaris 9/10 (sparc, ia32, x64);
- AIX 5/6 (Power PC). Только в исполнении 1.

3.3. Исполнения СКЗИ

Исполнение 1 СКЗИ класса **КС1** в составе криптопровайдера, криптодрайвера, модуля сетевой аутентификации (TLS) и сервисных программ; функционирует в программно-аппаратных средах, указанных в п. 3.2.

Исполнение 2 СКЗИ класса **КС2** в составе криптодрайвера, криптосервиса, модуля сетевой аутентификации (TLS), сервисных программ, утилиты выработки внешней гаммы; функционирует в программно-аппаратных средах, указанных в п. 3.2, за исключением среды AIX (Power).

3.4. Реализуемые криптографические алгоритмы

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

Алгоритмы формирования и проверки ЭЦП реализован в соответствии с ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".

Алгоритм выработки значения хэш-функции реализован в соответствии с 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 выработкой для каждого сеанса связи ключей на основе принципа открытого распределения ключей с использованием алгоритма Диффи-Хеллмана.

4. Структура и состав СКЗИ

4.1. Структура СКЗИ

Общая структура СКЗИ ЖТЯИ.00050-02 представлена на рис. 1.

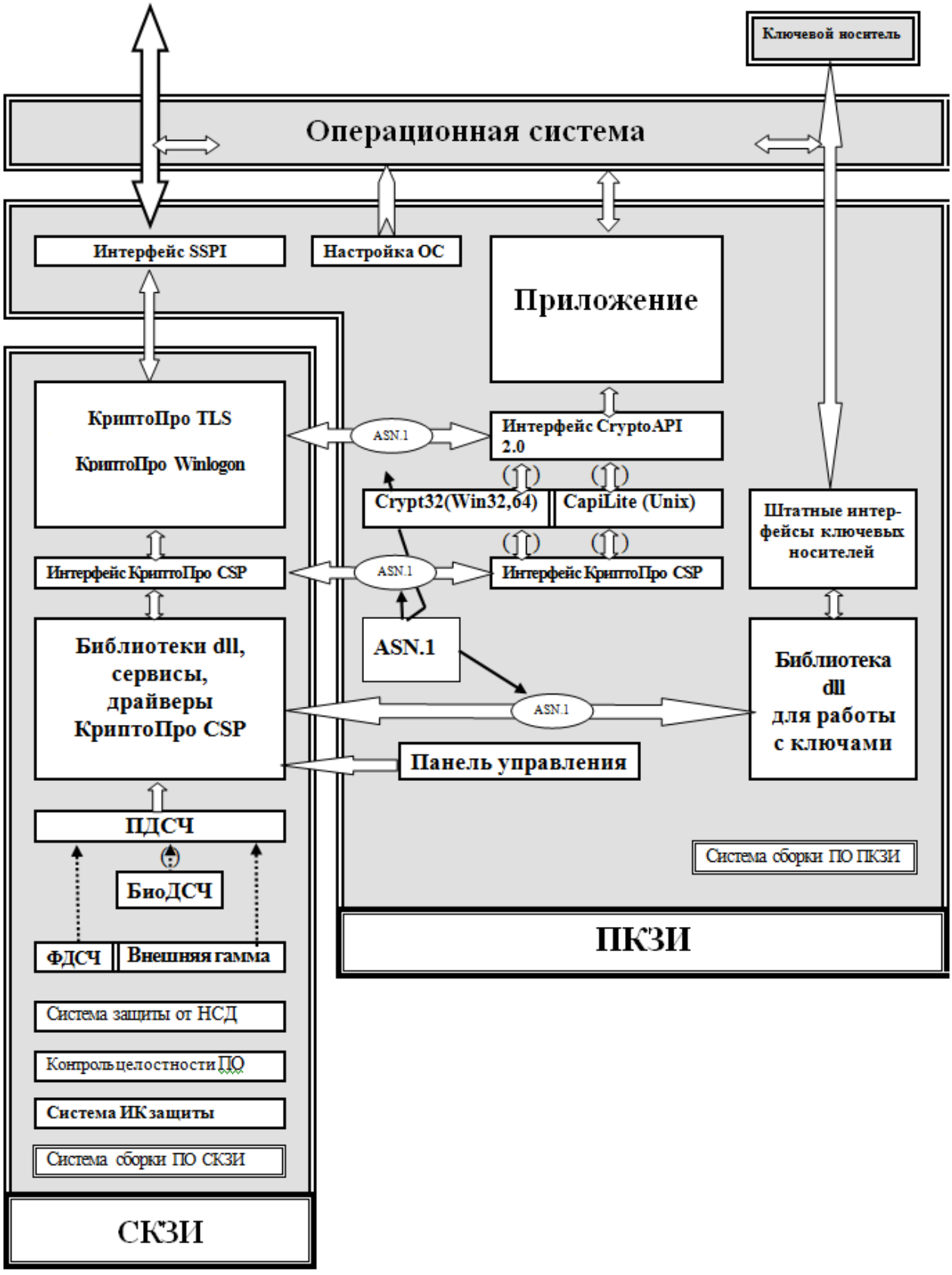


Рис. 1. Структура СКЗИ ЖТЯИ.00050-02

4.2. Состав СКЗИ

В состав СКЗИ ЖТЯИ.00050-02 входят:

- Библиотеки dll, сервисы, драйверы КриптоПро CSP.
- Модуль сетевой аутентификации КриптоПро TLS.
- Криптографический интерфейс КриптоПро CSP.
- Программный датчик случайных чисел (ПДСЧ). Инсталляция ПДСЧ в исполнении 1 = от БиоДСЧ или от внешней гаммы, в исполнении 2 - от физического ДСЧ (ФДСЧ) встраиваемого программно-аппаратного комплекса (ПАК) защиты от НСД, или от внешней гаммы.
- ПАК защиты от НСД. Используется в исполнении 2.
- Контроль целостности программного обеспечения.
- Система инженерно-криптографической защиты.
- Система защиты от НСД (используется опционально).

4.3. Состав ПКЗИ

В состав ПКЗИ входят следующие компоненты:

- Приложение (Прикладное программное обеспечение, использующее СКЗИ).
- Интерфейс SSPI (подмножество интерфейса криптографических протоколов Secure Support Provider Interface (SSPI, CryptoAPI v. 2.0) для реализации протокола сетевой аутентификации TLS v. 1.0 (под управлением ОС Windows2000/XP/2003/Vista/2008/7/2008R2).
- Модули настройки ОС Windows для обеспечения функционирования СКЗИ.
- Интерфейс CryptoAPI 2.0.
- Средства Crypt32(Win32,64) для обеспечения работы с сертификатами с использованием интерфейса CryptoAPI 2.0 через криптографический интерфейс КриптоПро CSP под управлением ОС Windows2000/XP/2003/Vista/2008/7/2008R2).
- Средства CapiLite - для обеспечения работы с сертификатами с использованием интерфейса CryptoAPI 2.0 через криптографический интерфейс КриптоПро CSP под управлением ОС семейства UNIX (Linux, FreeBSD, Solaris, AIX).
- Криптографический интерфейс КриптоПро CSP.
- Штатные интерфейсы ключевых носителей.
- ASN.1 - система кодирования/декодирования данных в форматах ASN.1.

Состав модулей СКЗИ и ПКЗИ конкретизируется в дополнениях [9]-[13] к данному документу.

5. Протокол 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:

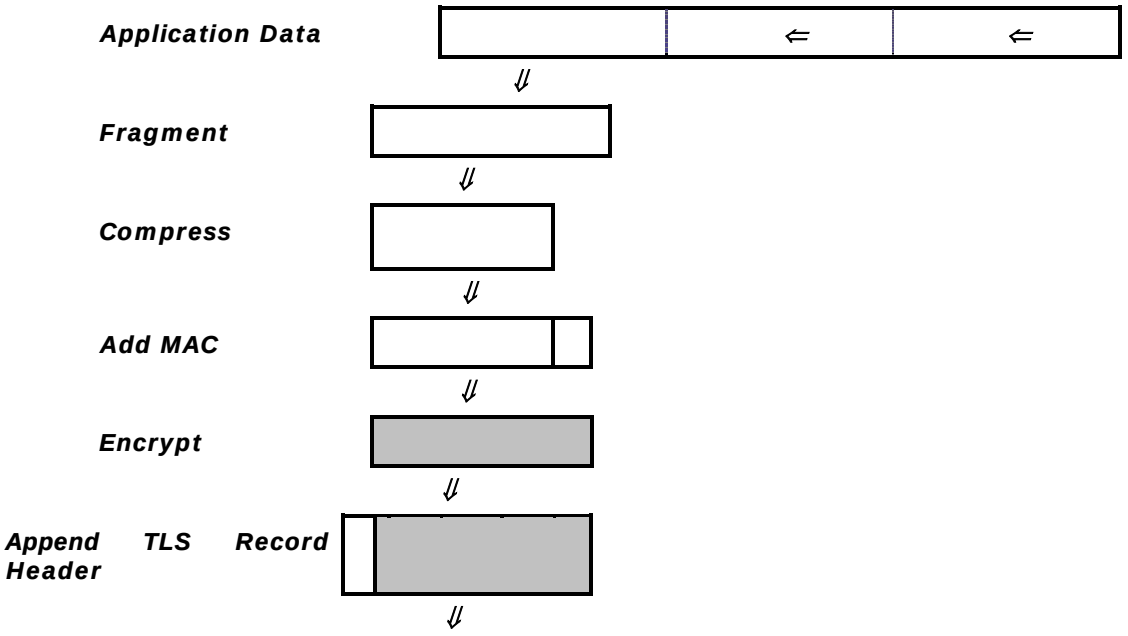
- Hello message (ClientHello, ServerHello);
- Change cipher specs message (изменение спецификации алгоритмов и параметров защиты);
- Key exchange message (передача ключа обмена ключами шифрования и MAC клиента, сервера);
- Alert message (предупреждение, оповещение о фатальной ошибке);
- Application_data 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:

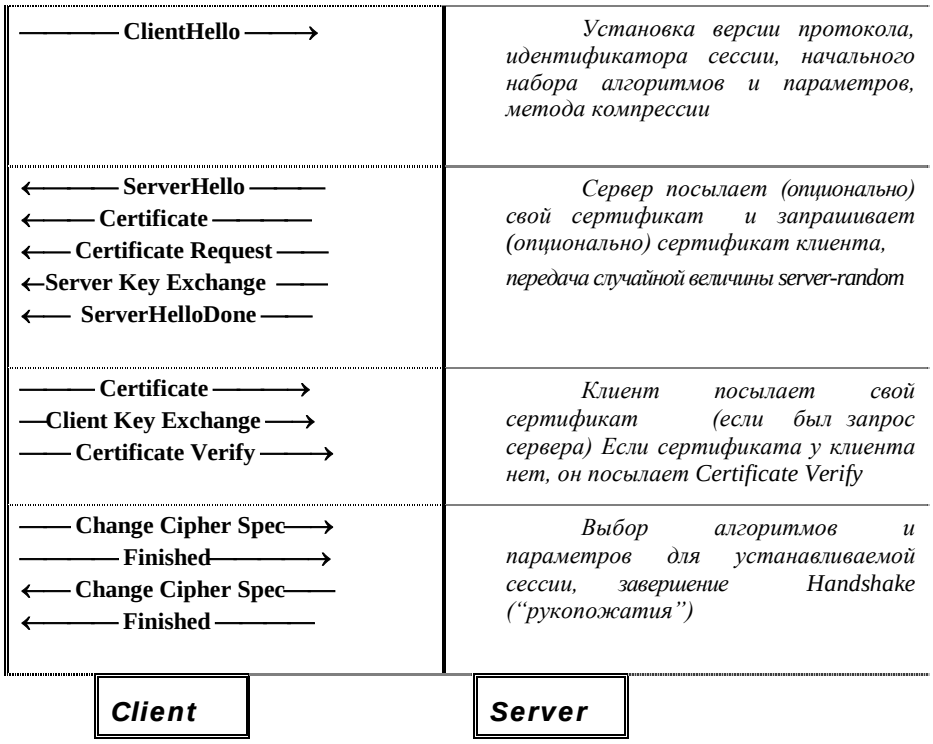
- компрессия фрагмента (опционально);
- вычисление хэша от конкатенации ключа хэширования, типа компрессии, длины компрессированного фрагмента, компрессированного фрагмента, заданной константы;
- шифрование расширенного фрагмента (конкатенация компрессированного фрагмента и его хэша);
- добавление открытого 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:



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.

<table>
<tr><td colspan="4">. . .</td></tr>
<tr><td>TLS Handshake Protocol</td><td>TLS Change Cipher Spec</td><td>TLS Alert Protocol</td><td>Протоколы обмена данными (HTTP и т.п.)</td></tr>
<tr><td colspan="4">TLS Record Protocol</td></tr>
<tr><td colspan="4">Транспортный протокол (TCP/IP и т.п.)</td></tr>
<tr><td colspan="4">. . .</td></tr>
</table>

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

На ПЭВМ клиента и на сервере (IIS, ISA) устанавливается СКЗИ ЖТЯИ.00050-02 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.

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

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

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

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

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.

Предупреждение. Алгоритм Диффи-Хеллмана обеспечивает формирование сеансовых ключей информационного обмена, но не обеспечивает аутентификацию связывающихся сторон. Поэтому данный алгоритм должен использоваться совместно с протоколами аутентификации.

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.00050-02 90 05 "КриптоПро CSP. Руководство программиста") 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. Для исполнения 1 закрытые ключи ЭЦП и шифрования формируются с использованием ПДСЧ с инициализацией его от БиоДСЧ или от внешней гаммы; для исполнения 2 - с использованием ПДСЧ с инициализацией его от физического ДСЧ ПАК защиты от НСД или от внешней гаммы. Для исполнения 2 с ОС Solaris 9/10 (платформа sparc) ключи должны быть получены на АРМ, оснащенных СКЗИ в исполнении 2 с ОС Windows XP, платформа ia32, и утилитой выработки гаммы.

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

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

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

6.5. Ключевые носители

Формирование закрытых ключей может производиться на ключевые носители:

- ГМД 3,5’’;
- USB диски
- электронный ключ с интерфейсом USB (e-Token);
- Смарткарты РИК, Оскар, Магистра
- идентификаторы Touch-Memory D S1995 – DS1996 ПАК защиты от НСД (Аккорд-АМДЗ, электронный замок "Соболь);
- Rutoken;
- Раздел HDD ПЭВМ (в ОС Windows – реестр).

Использование ключевых носителей в зависимости от программно-аппаратной платформы см. документ "ЖТЯИ.00050-02 30 01. СКЗИ "КриптоПро CSP". Формуляр, п.п. 3.8, 3.9.

Примечание 1. В состав дистрибутива СКЗИ ЖТЯИ.00050-02 входят библиотеки поддержки всех перечисленных носителей, но не входят драйвера для ОС. По вопросам получения драйверов необходимо обращаться к производителям соответствующих устройств.

Примечание 2. Допускается хранение закрытых ключей в реестре ОС Windows и в разделе HDD (в случае других ОС) при условии распространения на HDD или ПЭВМ с HDD требований по обращению с ключевыми носителями, в том числе и после удаления ключей из реестра.

Примечание 3. Вопрос об использовании в качестве ключевых носителей смарткарт других типов должен согласовываться с ООО "КРИПТО-ПРО".

6.6. Размеры ключей

Размеры ключей электронной цифровой подписи:

закрытый ключ – 256 бит;

открытый ключ – 512 бит.

Размеры ключей, используемых при шифровании:

закрытый ключ – 256 бит;

открытый ключ - 512 бит;

симметричный ключ – 256 бит.

6.7. Хранение ключевых носителей

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

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

При наличии в организации, эксплуатирующей СКЗИ, администратора безопасности и централизованном хранении ключевых носителей, администратор безопасности несет персональную ответственность за хранение личных ключевых носителей пользователей.

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

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

При хранении ключей на HDD ПЭВМ необходимо использовать парольную защиту.

СКЗИ может функционировать и хранить ключевую информацию в двух режимах:

- в памяти приложения для исполнения 1.
- в "Службе хранения ключей", реализованной в виде системного сервиса для исполнения 2.

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.

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

6.8. Сроки действия пользовательских ключей

При эксплуатации СКЗИ ЖТЯИ.00050-02 должны соблюдаться следующие сроки использования пользовательских закрытых ключей и сертификатов:

- максимальный срок действия закрытого ключа ЭЦП - 1 год 3 месяца;
- максимальный срок действия открытого ключа ЭЦП - 15 лет;
- максимальный срок действия закрытых и открытых ключей обмена – 1 год 3 месяца.

6.9. 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).

6.10. Интерфейс управления ключами СКЗИ

Последовательность действий при генерации закрытых ключей пользователей, управлении их паролями, управлении ключами определена в документе «ЖТЯИ.00050-02 90 03. КриптоПро CSP. Инструкция по использованию».

7. Требования по встраиванию и использованию ПО СКЗИ

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

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

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

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

1. Через интерфейс функций **CryptoAPI 2.0**, что позволяет применять весь инструментарий фирмы Microsoft. Для этих целей разработчики могут воспользоваться программной документацией, содержащейся в **MSDN (Microsoft Developer Network)**, а также поставляемым тестовым ПО; на Unix-платформах (Linux, FreeBSD 5, Solaris 10) через интерфейс библиотеки capilite.dll, являющейся подмножеством интерфейса **CryptoAPI 2.0.** Для этих целей **в комплект поставки включается документ ЖТЯИ.00050-02 90 05 "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.00050-02 90 05 "КриптоПро CSP. Руководство программиста", описывающий состав функций и тестовое ПО.

Ниже приведен основной перечень требований и условий по встраиванию, реализуемых при использовании СКЗИ.

7.1. Конфиденциальность информации

При передаче данных в сети обеспечивается использованием функций шифрования.

Для обеспечения защиты от 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). 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, повтора 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, средств антивирусной защиты и организационных мероприятий.

7.9. Правила встраивания и использования СКЗИ

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

1. При использовании открытого ключа должны быть обеспечены его авторизация, достоверность, целостность и идентичность. 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 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
}
```

7.10. Использование расширенного интерфейса СКЗИ

Внешний интерфейс СКЗИ ЖТЯИ.00050-02 позволяет использовать более широкий по сравнению с предыдущими версиями класс криптографических протоколов, построенных на базе СКЗИ (в частности, криптографические протоколы, обеспечивающие использование работы СКЗИ с функциональным ключевым носителем (ФКН), протоколы IPSec и др.).

8. Управление ключами СКЗИ

Ключевая система СКЗИ базируется на архитектуре PKI рекомендаций X509 и в части управления сертификатами открытых ключей должна обеспечиваться Удостоверяющим центром (УЦ). В качестве УЦ может выступать Удостоверяющий центр КриптоПро УЦ, но допускается использование Центра Сертификации корпорации Microsoft (Microsoft Certification Authority), или другие реализации, обеспечивающие выполнение функций доверенного обращения с сертификатами.

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

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

Описание Удостоверяющего центра КриптоПро УЦ приведено в Приложении 4.

Примечание.

СКЗИ ЖТЯИ.00050-02 может использоваться в качестве криптоядра в составе различных прикладных систем, организационные схемы управления ключевой системой которых могут отличаться от рассматриваемой.

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

8.1. Удостоверяющий центр

Удостоверяющий центр обеспечивает выполнение следующих функций:

- регистрация (формирование) дистрибутивов ПО СКЗИ и выдача их пользователям;
- формирование, хранение и использование закрытого ключа (ключей) Центра Сертификации;
- регистрация пользователей в соответствии с требованиями Регламента (Договора) системы;
- получение от пользователя запроса на сертификат, как в электронном, так и в бумажном виде;
- верификация запроса на сертификат;
- формирование сертификатов открытых ключей 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 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. [23]).

8.2.1. Закрытый ключ и сертификат ЦС

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

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

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. 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. Пользователь системы или администратор безопасности прибывают в Центр Регистрации УЦ 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. 3. 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. 3. 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. Формирование личных ключей пользователя

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

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

2. Пользователь производит формирование личного 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".

8.5.3. Получение личного сертификата пользователем

Личный сертификат может быть получен следующими способами:

- при личном присутствии пользователя (администратора безопасности) в УЦ;
- по сети с использованием зарегистрированного адреса электронной почты или в процессе непосредственного соединения с центром.

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

При передаче личного сертификата пользователю ему 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 понятия.

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".

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. Разбор 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 РФ 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.	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 хранящегося в нем ключа. Порядок действий при компрометации ключей описан в разделе 8.8.3 "Компрометация ключей пользователя".
	Отказы и сбои в работе программных средств вследствие не выявленных ранее ошибок в	При отказах и сбоях в работе программных средств, в следствии не выявленных ранее ошибок в программном обеспечении, необходимо остановить работу, локализовать по возможности причину отказов и сбоев и вызвать разработчика данного ПО

№ п/п	Нештатная ситуация	Действия персонала
	программном обеспечении.	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).

11. Требования по НСД

11.1. Общие требования по организации работ по защите от НСД

Защита аппаратного и программного обеспечения от НСД при установке и использовании СКЗИ является составной частью общей задачи обеспечения безопасности информации в системе, в состав которой входит СКЗИ.

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

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

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

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

Администратор безопасности не должен иметь возможность доступа к конфиденциальной информации пользователей.

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

11.2. Требования по размещению технических средств с установленным СКЗИ.

При размещении технических средств с установленным СКЗИ:

- Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию.
- Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ, сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.
- Размещение СКЗИ ЖТЯИ.00050-02 в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осущест-вляется установленным порядком.

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

1. ПЭВМ, на которых используется СКЗИ, должны быть допущены для обработки конфиденциальной информации по действующим в Российской Федерации требованиям по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К), с учетом модели угроз в информационной системе заказчика, которым должно противостоять СКЗИ ЖТЯИ.00050-02.

2. Инсталляция СКЗИ ЖТЯИ.00050-02 на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.

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

При установке программного обеспечения СКЗИ следует:

- На технических средствах, предназначенных для работы с СКЗИ, использовать только лицензионное программное обеспечение фирм - изготовителей.
- При установке ПО СКЗИ на ПЭВМ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ и совместно поставляемых с СКЗИ компонент СФК.
- На ПЭВМ не должны устанавливаться средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти СКЗИ и приложений, использующих СКЗИ, а также для просмотра кода и памяти СКЗИ и приложений, использующих СКЗИ, в процессе обработки СКЗИ защищаемой информации и/или при загруженной ключевой информации.
- Предусмотреть меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлены СКЗИ (например, путем опечатывания системного блока и разъемов ПЭВМ).
- После завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО СКЗИ, а также его окружения в соответствии с документацией.
- Программное обеспечение, устанавливаемое на ПЭВМ с СКЗИ не должно содержать возможностей, позволяющих:
  - модифицировать содержимое произвольных областей памяти;
  - модифицировать собственный код и код других подпрограмм;
  - модифицировать память, выделенную для других подпрограмм;
  - передавать управление в область собственных данных и данных других подпрограмм;
  - несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;

- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

11.4. Меры по обеспечению защиты от НСД

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

- Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:
- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п .);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.

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

ЗАПРЕЩАЕТСЯ:

- оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;
- записывать на ключевые носители постороннюю информацию;

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

- не использовать нестандартные, измененные или отладочные версии ОС.
- исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой.
- исключить возможность удаленного управления, администрирования и модификации ОС и её настроек.
- на ПЭВМ должна быть установлена только одна операционная система.
- правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности.
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.).
- режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень.
- всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.

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

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

Кроме того, необходимо организовать стирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

• должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии.

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

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

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

• организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.

• организовать и использовать комплекс мероприятий антивирусной защиты.

• должно быть запрещено использование СКЗИ для защиты речевой информации.

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

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

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).

11.5. Использование СКЗИ со стандартными программными средствами СФК

Программное обеспечение СКЗИ ЖТЯИ.00050-02 позволяет использовать российские криптографические алгоритмы и сертификаты открытых ключей стандарта X.509 с различным программным обеспечением Microsoft:

- Центр Сертификации - Microsoft Certification Authority, входящий в состав Windows 2000 Server, Advanced Server, Windows 2003 Server, Windows 2008 Server, Windows 2008r2.
- Электронная почта - MS Outlook (Office 2007, Office 2003, Office XP, Office 2000).
- Электронная почта - Microsoft Outlook Express в составе Internet Explorer.
- Microsoft Word, Excel, Info Path из состава Microsoft Office 2003, 2007.
- Средства контроля целостности ПО, распространяемого по сети - Microsoft Authenticode.
- Службы терминалов для Windows 2003 Server, Windows 2008 Server, Windows 2008r2 Server (включая шлюз служб терминалов).
- Защита TCP/IP соединений в сети Интернет - протокол TLS/SSL при взаимодействии Internet Explorer – web-сервер IIS, TLS-сервер, TLS-клиент (IE).
- SQL-сервер.
- ISA сервер.
- Сервер терминалов и клиент (RDP).
- Средства функционирования комплекса разработки ООО «КРИПТО-ПРО» Крипто-Про УЦ 1.4, КриптоПро OCSP, КриптоПро TSP, КриптоАРМ, CryptCP, Клиент КриптоПро HSM.

СКЗИ ЖТЯИ.00050-02 при функционировании под управлением ОС Windows может использоваться с дополнительными программными средствами защиты:

ЖТЯИ.00032-01 30 01. КриптоПро Winlogon. Средство сетевой аутентификации.

ЖТЯИ.00051-01 30 01. КриптоПро EFS. Средство хранения конфиденциальной информации.

Под управлением UNIX-подобных ОС СКЗИ ЖТЯИ.00050-02 используется с программным обеспечением:

- Certmgr (КриптоПро Certmgr).
- CryptCP.
- Apache Trusted TLS (Digt).
- Trusted TLS (Digt).

Программное обеспечение СКЗИ ЖТЯИ.00050-02 совместимо со средствами антивирусной защиты:

- McAfee VirusScan Enterprise Version 8.0i.
- Norton (Symantec) Antivirus.
- Антивирус Касперского
- Антивирус NOD32.

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

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

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

- Порядок подключения СКЗИ к каналам.
- Выделено лицо, ответственное за безопасность работы по общедоступным каналам.
- Разработан типовой регламент защищенной связи, включающий:
  - политику безопасности защищенной связи.

- допустимый состав прикладных программных средств, для которого должно быть исследовано и обосновано отсутствие негативного влияния на СКЗИ по каналу передачи данных.
- перечень допустимых сетевых протоколов.
- защиту сетевых соединений (перечень допустимых сетевых экранов).
- система и средства антивирусной защиты.

3. Перечень стандартных программных средств, приведенных в п. 11.5, может включаться администратором в типовой регламент без проведения дополнительных исследований. При этом должны выполняться:

- своевременное обновление программных средств, включенных в состав регламента.
- контроль среды функционирования СКЗИ.
- определение и контроль за использованием сетевых протоколов.
- соблюдение правил пользования СКЗИ и средой функционирования СКЗИ.

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

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

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

В качестве программно-аппаратных средств защиты от НСД в СКЗИ могут использо-ваться Программно-аппаратный комплекс "Аккорд-АМДЗ" и электронный замок "Соболь". Идентификационные данные указанных средств приведены в документе "ЖТЯИ.00050-02 3 0 01. КриптоПро CSP. Формуляр", п.3, Примечание 2.

11.7.1. Программно-аппаратный комплекс "Аккорд-АМДЗ"

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

ПАК "Аккорд-АМДЗ" используется на платформах

- Windows (платформа IA32);
- Linux (платформа IA32);
- FreeBSD 6/7 (платформа IA32);
- Solaris 9/10 (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".

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.

11.7.2. 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.

Электронный замок "Соболь" используется на платформах

- Windows (платформа IA32);
- Linux (платформа IA32);
- FreeBSD 6/7 (платформа IA32);
- Solaris 9/10 (платформа IA32).

Электронный замок "Соболь" обеспечивает:

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

Установка и настройка электронного замка на АРМ пользователя должна производиться в соответствии с эксплуатационной документацией. Перед эксплуатацией электронного замка в составе АРМ пользователя необходимо ознакомиться с комплектом документации (в соответствии с паспортом УВАЛ.00300-04 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.

11.8. О возможности использования СКЗИ ЖТЯИ.00050-02 с дополнительными программными средствами защиты

СКЗИ ЖТЯИ.00050-02 при функционировании под управлением ОС Windows может использоваться с дополнительными программными средствами защиты:

1. КриптоПро Winlogon. Средство сетевой аутентификации. ЖТЯИ.00032-01 30 01, Формуляр.
2. КриптоПро EFS. Средство хранения конфиденциальной информации. ЖТЯИ.00051-01 30 01. Формуляр.

12. Требования по криптографической защите

Должны выполняться требования по криптографической защите:

1. Использование только лицензионного системного программного обеспечения.
2. Настройки операционных систем для работы с СКЗИ, включенные в документы ЖТЯИ.00050-02 90 02-01, ЖТЯИ.00050-02 90 02-02, ЖТЯИ.00050-02 90 02-03, ЖТЯИ.00050-02 90 02-04, ЖТЯИ.00050-02 90 02-05.
3. При инсталляции СКЗИ должны быть обеспечены организационно-технические меры по исключению подмены дистрибутива и внесения изменений в СКЗИ после установки.
4. Исключение из программного обеспечения ПЭВМ с установленным СКЗИ средств отладки.
5. СКЗИ должно использоваться со средствами антивирусной защиты, сертифицированными по требованиям ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.
6. Ключевая информация является **конфиденциальной**.
7. Внешняя гамма, используемая для инициализации состояния программного ДСЧ, является **конфиденциальной**.

8. Пароль, используемый для аутентификации пользователей, должен содержать не менее 6 символов алфавита мощности не менее 10. Периодичность смены пароля – не реже одного раза в 3 месяца.

9. Периодичность тестового контроля криптографических функций - 10 минут.

10. Ежесуточная перезагрузка ПЭВМ.

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

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

13. Должно даваться предупреждение о том, что при использовании режима шифрования CRYPT_SIMPLEMIX_MODE материал, обрабатываемый на одном ключе, автоматически ограничивается величиной 4 MB.

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

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

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

17. При функционировании исполнения 2 СКЗИ в программно-аппаратных средах Windows XP/2003 (ia64), ОС Solaris 9 /10 (sp arc, i a32, x 64) инициализация ПДСЧ должна производиться с использованием внешней гаммы.

18. При функционировании исполнения 2 СКЗИ в программно-аппаратных средах Windows (x64, ia64), Solaris 9/10 (sparc, x64), для которых в настоящее время нет работающих с ними ПАК защиты от НСД, должны выполняться организационно-технические меры, исключающие возможность несанкционированного доступа к конфиденциальной информации в открытом виде и обеспечено ее хранение в ПЭВМ только в виде, зашифрованном на ключах пользователей.

19. Контролем целостности должны быть охвачены файлы, указанные в разделах «Требования по криптографической защите» документов ЖТЯИ.00050-02 90 02-01, ЖТЯИ. 00050-02 90 02-02, ЖТЯИ.00050-02 90 02-03, ЖТЯИ.00050-02 90 02-04, ЖТЯИ.00050-02 90 02-05.

20. **ЗАПРЕЩАЕТСЯ** использование беспроводных компьютерных мышей.

Литература

1. Закон РФ "Об электронной цифровой подписи", 10 января 2002 г. № 1-ФЗ.
2. Закон РФ "Об информации, информационных технологиях и о защите информации", 27 июля 2006 года № 149-ФЗ.
3. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
4. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
5. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.
6. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).
7. ЖТЯИ.00050-02 30 01. КриптоПро CSP. Формуляр.
8. ЖТЯИ.00050-02 90 01. КриптоПро CSP. Описание реализации.
9. ЖТЯИ.00050-02 90 0 2-01. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows.
10. ЖТЯИ.00050-02 90 0 2-02. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС в ОС Linux.
11. ЖТЯИ.00050-02 90 0 2-03. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС FreeBSD.
12. ЖТЯИ.00050-02 90 0 2-04. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Solaris.
13. ЖТЯИ.00050-02 90 0 2-05. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС AIX.
14. ЖТЯИ.00050-02 90 03. СКЗИ "КриптоПро CSP". Инструкция по использованию.
15. ЖТЯИ.00050-02 90 04. СКЗИ "КриптоПро CSP". АРМ выработки внешней гаммы.
16. ЖТЯИ.00050-02 90 05. КриптоПро CSP. Руководство программиста.
17. ЖТЯИ.00035-01 30 01. Удостоверяющий центр "КриптоПро УЦ". Формуляр.
18. OSI NETWORKING AND SYSTEM ASPECTS. Abstract Syntax Notation One (ASN.1)
19. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.
20. RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.
21. RFC 3369, "Cryptographic Message Syntax", August 2002.
22. RFC 4357, "Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms".
23. RFC 4490, "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)".
24. RFC 4491, "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

Приложение 1. Акт готовности к работе

УТВЕРЖДАЮ

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

АКТ

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

"_____" _____ 201___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	21.01.2010		Администратор безопасности
2		Иванов И. И.	Почтовый адрес: a.sidorov@acme.ru Должность:	01.02.2010		Оператор расчетной системы

Приложение 3. Журнал пользователя сети

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

Приложение 4.«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;
- Ведение 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

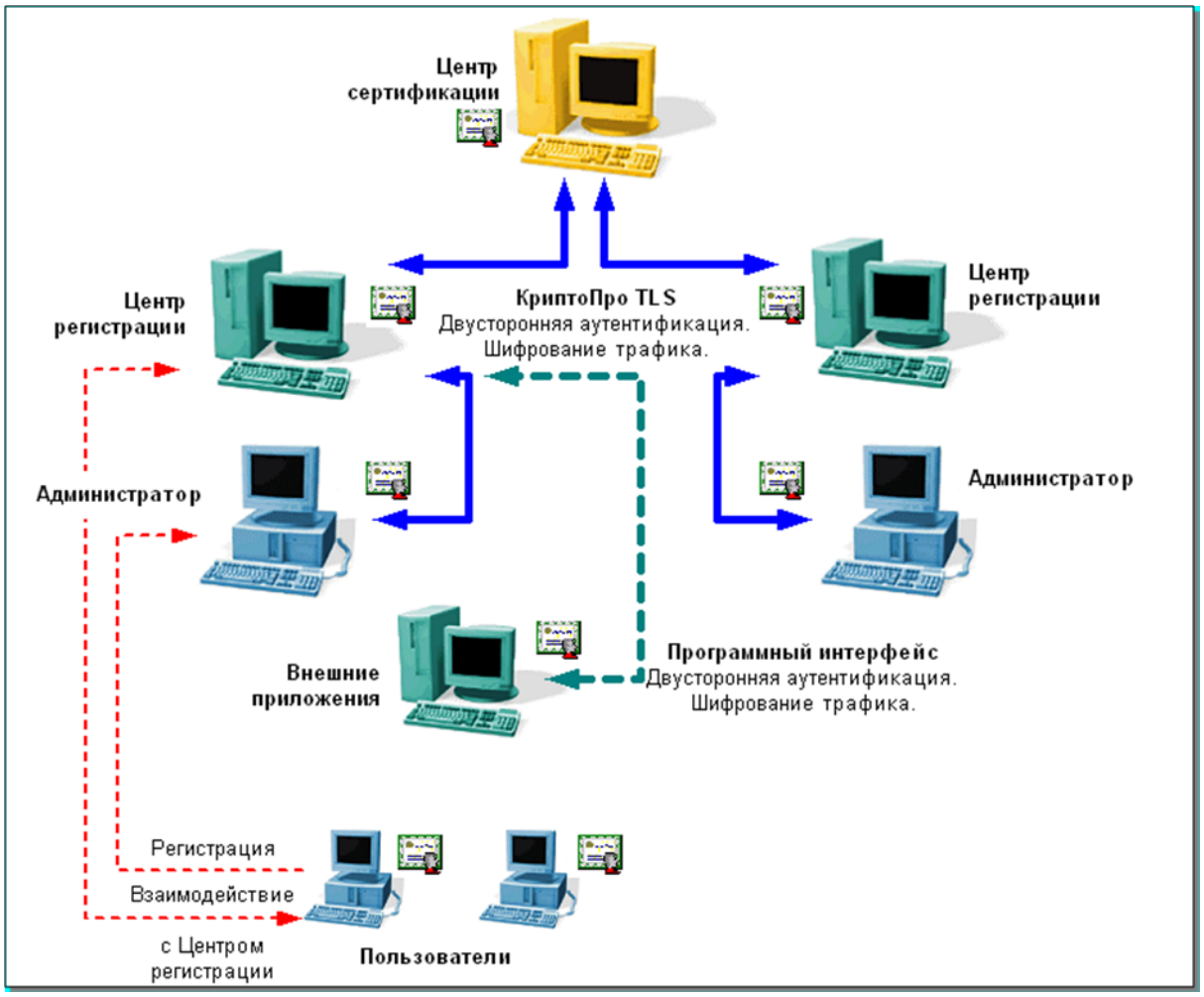
  - Управление оповещением пользователей о событиях в процессе регистрации;

  - Управление оповещением пользователей о событиях в течении всего жизненного цикла сертификатов открытых ключей.

Архитектура ПК «КриптоПро УЦ»

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

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



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 2000/2003 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 2000/2003 Server и использует базу данных Microsoft SQL 2000 Server (Desktop Edition, Standard Edition или Enterprise Edition). M icrosoft S QL 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/XP/2003. 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/XP/2003. 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 O bject A ccess P rotocol) —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 D escription, D iscovery a nd I ntegration) — 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 ПК «КриптоПро УЦ»

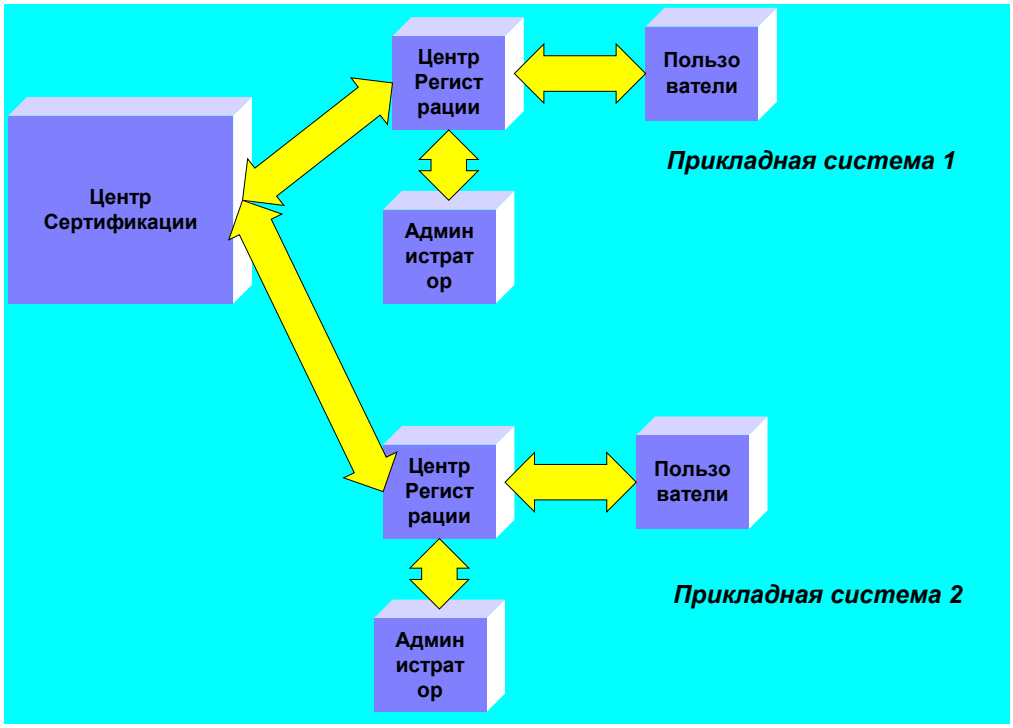
Масштабируемость

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

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

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

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



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

Производительность

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

Лист регистрации изменений

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