127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
https://CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро CSP Версия 5.0 KC1 1-Base

Руководство администратора безопасности. Общая часть

ЖТЯИ.00101-01 91 01
Листов 38

2019 г

Содержание

Аннотация

Настоящее Руководство содержит общее описание средства криптографической защиты информации КриптоПро CSP версия 5.0 КС1 Исполнение 1-Base (ЖТЯИ.00101-01) и рекомендации по использованию СКЗИ в различных автоматизированных системах.

В зависимости от комплектации и используемой программно-аппаратной среды функционирования СКЗИ следует руководствоваться также документами [1—17].

Инструкции администратора безопасности и пользователя различных автоматизированных систем, использующих КриптоПро CSP версии 5.0 КС1, должны разрабатываться с учетом требований настоящего Руководства.

Список определений и сокращений

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

Основные термины и понятия

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

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

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

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

Администратор безопасности
Субъект доступа, основной обязанностью которого является обеспечение безопасности конфиденциальной связи на том участке сети, которую он курирует.

Система административного управления безопасностью включает в себя комплекс организационно-технических мер, направленных на обеспечение конфиденциальности связи.

Основные направления деятельности администратора безопасности:
- контроль целостности программного обеспечения;
- управление ключевой системой: хранение, ввод в действие и смена ключей пользователей, генерация закрытых и открытых ключей подписи пользователей, ключей электронной подписи, ключей проверки электронной подписи;
- управление доступом пользователей системы к программному обеспечению и данным, включая установку и периодическую смену паролей, управление средствами защиты коммуникаций, передаваемых, хранимых и обрабатываемых данных.

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

Аутентификация
Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

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

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

Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба.

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

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

Блокирование информации

Прекращение или затруднение доступа законных пользователей к информации.

Верификация

Установление соответствия принятой и переданной информации с помощью логических методов.

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

Владелец информации, информационной системы

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.

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-разыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

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 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, ARM, ARM64, ARMv7, MIPS, Эльбрус

Аппаратные платформы, используемые производителями ПЭВМ

Идентификация

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

Имитозащита

Защита системы шифрованной связи от навязывания ложных данных.

Имитовставка

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

Квалифицированный сертификат ключа проверки электронной подписи

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

Ключ (криптографический ключ)

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

Ключ проверки электронной подписи

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

Ключ электронной подписи

Уникальная последовательность символов, предназначенная для создания электронной подписи.

Компрометация ключа

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

1) Потеря ключевых носителей.
2) Потеря ключевых носителей с их последующим обнаружением.
3) Увольнение сотрудников, имевших доступ к ключевой информации.
4) Нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа.
5) Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
6) Нарушение печати на сейфе с ключевыми носителями.

7) Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)

Различаются два вида компрометации закрытого ключа: 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, создания и проверки подписи, генерации пользовательских ключей. Обеспечивает работу с сессионными ключами шифрования (генерация, экспорт/импорт в защищенном виде), закрытыми и открытыми ключами ЭП и обмена, ввод ключей с ключевых носителей, защищённое хранение и уничтожение ключей в оперативной памяти. Реализуется как библиотека, динамически загружаемая в единое адресное пространство процесса, инициируемого прикладной задачей.

Криптодрайвер

Реализует функции шифрования и вычисления имитовставки, хэширования и проверки подписи. Обеспечивает работу с сессионными ключами шифрования (генерация, экспорт/импорт в защищенном виде), ключами проверки ЭП, эфемерными закрытыми и открытыми ключами обмена, защищённое хранение и уничтожение ключей в оперативной памяти. Загружается в адресное пространство ядра ОС. По своему интерфейсу и функциональным возможностям криптодрайвер обеспечивает возможности криптопровайдера за исключением функций создания электронной подписи, работы с носителем ключей, генерации ключей пользователя. Позволяет организовывать шифрование данных и проверку цифровой подписи на уровне ядра операционной системы и ускорить криптографические операции с потоком данных за счет исключения из процесса обработки данных их пересылку с уровня ядра на уровень приложений и обратно.

Криптосервис

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

Криптографическое преобразование

Преобразование информации с использованием криптографических алгоритмов.

Лицензирование в области защиты информации

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

Мероприятия по защите информации

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

Мероприятия по контролю эффективности защиты информации

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

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

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

Нарушитель правил разграничения доступа
Субъект доступа, осуществляющий несанкционированный доступ к информации.

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

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

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

Несанкционированный доступ к информации (НСД)
Получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

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

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

Обработка информации
Передача, прием, хранение, преобразование и отображение информации.

Организация защиты информации
Содержание и порядок действий по обеспечению защиты информации.

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

Пароль

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

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

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

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.

Пользователь (потребитель) информации

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

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

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

Проверка электронной подписи документа

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

Разглашение

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

Расшифрование данных

Процесс преобразования зашифрованных данных в открытые данные при помощи шифра.

Регламентация

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

Санкционированный доступ к информации

Доступ к информации, не нарушающий правила разграничения доступа.

Сертификат защиты

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

Сертификат ключа проверки электронной подписи

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

Сертификат открытого ключа

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

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

Формат сертификата определен в рекомендациях ITU-T X.509 и рекомендациях IETF RFC 5280. В настоящее время основным принятым форматом является формат версии 3, позволяющий определить дополнения (extensions), с помощью которых реализуется определенная политика безопасности в системе.

Сертификат соответствия

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

Секретный (закрытый) ключ

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

Система защиты информации

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

Система защиты информации от НСД

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

Служебная и коммерческая тайна

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.

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

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.

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

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

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.

К основным способам НСД относятся:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая осуществить НСД;
- внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

Средства вычислительной техники

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

Средство защиты информации

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

Средство защиты от несанкционированного доступа

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

Средство криптографической защиты информации

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

Субъект доступа

Лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Субъект информационных отношений

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

Техническое средство обработки информации

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

Угроза безопасности

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

Удостоверяющий центр

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

Уничтожение информации

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

Управление ключами

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

Утечка информации

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

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

Функция хэширования

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

Целостность информации

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

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

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.

Рисунок 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

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

1) средства шифрования — аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;
2) средства имитозащиты — аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации;
3) средства электронной подписи;
4) средства кодирования — средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций;
5) средства изготовления ключевых документов — аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств;
6) ключевые документы — электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах;
7) аппаратные шифровальные (криптографические) средства — устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин;

8) программные шифровальные (криптографические) средства — программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств;
9) программно-аппаратные шифровальные (криптографические) средства — устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.

Шифрующая файловая система

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

Электронная подпись

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

Данные, добавляемые к блоку данных полученные в результате его криптографического преобразования, зависящего от ключа ЭП и блока данных, которые позволяют приемнику данных удостовериться в целостности блока данных и подлинности источника данных, а также обеспечить защиту от подлога со стороны приемника данных. Проверка электронной подписи под блоком открытой информации производится с помощью криптографического преобразования и открытого ключа (ключа проверки ЭП), соответствующего закрытому (ключу ЭП), участвовавшего в процессе установки ЭП.

Рисунок 2. Создание и проверка ЭП

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

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

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

1 Назначение СКЗИ

СКЗИ КриптоПро CSP версии 5.0 КС1 представляет собой программный комплекс, предназначенный для реализации широкого набора решений по обеспечению криптографическими методами (основанными на государственных стандартах РФ) информационной безопасности на отдельных рабочих местах, в архитектуре «клиент-сервер», а также в информационных и телекоммуникационных системах различного назначения.

СКЗИ КриптоПро CSP может выступать как в качестве готового к применению средства, так и в качестве платформы для построения на его основе программных, программно-аппаратных и аппаратных решений в области обеспечения информационной безопасности, основанных на применении российских криптографических алгоритмов.

СКЗИ предназначено для выполнения следующих функций:

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

2) шифрование, вычисление имитовставки, хэширование, создание/проверка ЭП;

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

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

5) защита IP-соединений («КриптоПро IPsec»).

2 Протокол сетевой аутентификации «КриптоПро TLS»

Модуль поддержки сетевой аутентификации позволяет реализовать защищенный сетевой протокол в соответствии с рекомендациями [18, 19]. Модуль обеспечивает двустороннюю и одностороннюю аутентификацию приложений при их взаимодействии по сети с использованием алгоритма ЭП и сертификатов открытых ключей, а также шифрование данных, передаваемых в сетевом соединении.

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

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

Для подключения по протоколу TLS используется префикс https, при этом обозреватель Web-сервера по умолчанию будет подключаться к порту TCP 443 вместо стандартного порта TCP 80. Если сервер не поддерживает протокол TLS, соединение не устанавливается. Применение протоколов SSL/TLS (SSL - более ранние версии протокола) показано в табл. 1.

Таблица 1. Применение протокола SSL/TLS

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

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

В процессе взаимной аутентификации:

- выполняется криптографическая проверка наличия у сервера закрытого ключа, соответствующего открытому ключу, указанному в сертификате;
- проверяется степень доверия издателю сертификата;
- проверяется, не истек ли срок действия сертификата;
- проверяется, не отозван ли сертификат; по умолчанию Internet Explorer/Microsoft Edge эту проверку не выполняет — это делает IIS.

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

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

2.1 Основные понятия протокола TLS

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

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

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

Сессия характеризуется следующими атрибутами:
- идентификатор сессии (случайное число, 32 байта, задается сервером при открытии сессии);
- метод компрессии;
- сертификат сервера (опционально);
- сертификат клиента (опционально);
- спецификация алгоритмов и параметров защиты (алгоритмы шифрования и MAC, криптографические параметры);
- master secret (используется при генерации ключей шифрования, ключей MAC, векторов инициализации);
- флаг, разрешающий/запрещающий новые соединения в сеансе.

Сертификаты представляются в стандарте X.509 v3. Спецификация алгоритмов и параметров защиты может меняться в течение сессии.

Соединение характеризуется следующими атрибутами:
- client_random — случайные 32 байта, задаваемые клиентом;
- server_random — случайные 32 байта, задаваемые сервером;
- client write MAC secret (ключ клиента для вычисления значения ключевой хэш-функции);
- server write MAC secret (ключ сервера для вычисления значения ключевой хэш-функции);
- client write key (ключ, используемый для шифрования данных клиентом и расшифрования их сервером);
- server write key (ключ, используемый для шифрования данных сервером и расшифрования их клиентом);
- client write IV, server write IV (векторы инициализации, используемые клиентом и сервером соответственно);
- порядковый номер соединения (поддерживается независимо для передаваемых и принимаемых сообщений).

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

Порядковые номера соединений поддерживаются независимо для передаваемых и принимаемых сообщений. При смене сессии, изменении спецификации алгоритмов и параметров защиты нумерация соединений начинается с 0; диапазон нумерации: $0 \div 2^{64}$-1.

Соединение ассоциируется с одной сессией.

Алгоритм преобразования информации при обмене с использованием протокола TLS включает следующие операции:
- прием от протокола верхнего уровня потока не интерпретируемых данных в блоках произвольного размера;
- фрагментация принятых с верхнего уровня данных в структурированные блоки (фрагменты) протокола TLS. Размер фрагмента – не более 214 байт;
- компрессия фрагментов (опционально);
- вычисление значения ключевой хэш-функции (MAC) от конкатенации ключа хэш-функции, типа компрессии, длины компрессированного фрагмента, компрессированного фрагмента и заданной константы;
- конкатенация фрагмента и результата вычисления значения хэш-функции от него (расширенный фрагмент);
- зашифрование расширенного фрагмента (опционально);
- добавление открытого заголовка, содержащего тип сообщения (один байт), версию протокола TLS (два байта) и длину компрессированного фрагмента.

Схема алгоритма представлена на рис. 3.

При приеме информации применяется обратная последовательность операций.

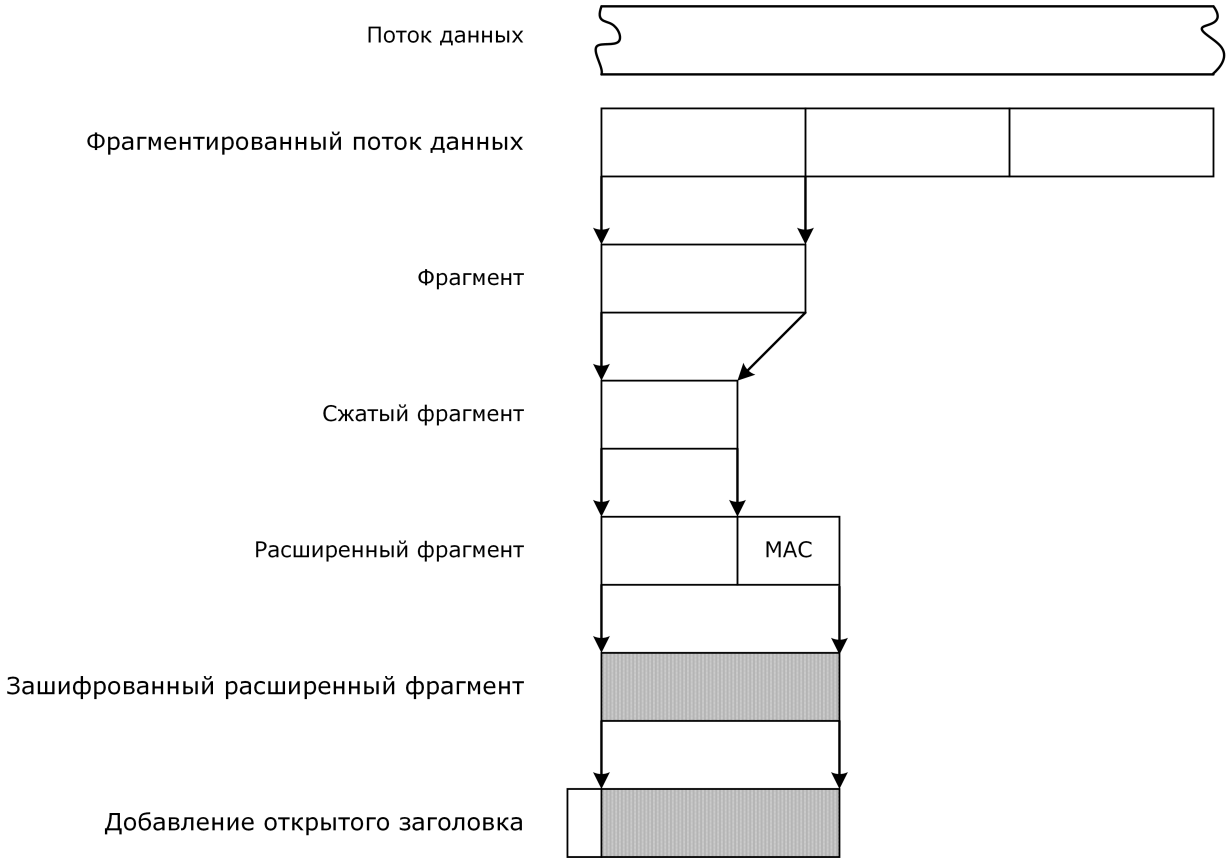


Рисунок 3. Алгоритм преобразования информации при обмене с использованием протокола TLS

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

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

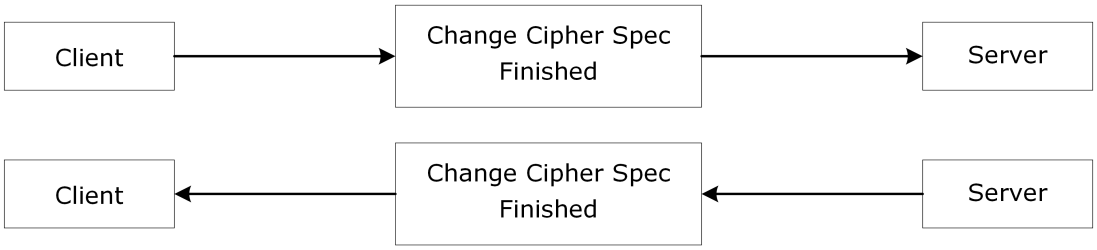
TLS Handshake Protocol обеспечивает инициализацию сессии (соединения) выполнением следующих операций:
- клиент и сервер договариваются об используемых в сессии алгоритмах и параметрах защиты, обмениваются случайными величинами client_random, server_random, договариваются, будут или нет новые соединения;
- производится обмен сертификатами для аутентификации клиента и сервера (по заданным опциям);
- клиент генерирует случайную величину pre_master secret, шифрует ее и передает серверу.
- клиент и сервер по pre_master secret, client_random и server_random формируют master secret (набор необходимой ключевой информации) сессии.

TLS Handshake Protocol работает по схеме, представленной на рис. 4.

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

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

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



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

Рисунок 4. Схема работы TLS Handshake Protocol

2.2 Модуль сетевой аутентификации «КриптоПро TLS»

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

Аутентификация клиент-сервер может быть односторонней и двусторонней.

Односторонняя аутентификация обеспечивает минимально необходимый уровень защиты, и включает в себя:
- обязательную аутентификацию сервера без аутентификации клиентов;
- шифрование трафика между клиентом и сервером.

При работе в данном режиме сервер на этапе «рукопожатия» не запрашивает сертификат клиента и устанавливается «анонимное» защищенное соединение. В этом случае клиент может не иметь закрытого ключа и

сертификата, однако при этом он лишается возможности создать электронную подпись под документами. Режим с односторонней аутентификацией сервера может использоваться для предоставления некоторой группе пользователей конфиденциальной информации на основании парольной защиты, однако пароль в этом случае будет предъявляться пользователем только после установления защищенного TLS-соединения с Web-сервером, что повышает уровень защиты от несанкционированного доступа по сравнению с передачей пароля по открытым соединениям. При односторонней аутентификации сервер запрашивает сертификат клиента, но его отсутствие не считается ошибкой.

Двусторонняя аутентификация включает в себя:
- взаимную аутентификацию клиента и Web-сервера с помощью их сертификатов;
- шифрование трафика между клиентом и сервером;
- создание и проверку электронной подписи под электронными HTML-формами, заполняемыми пользователями.

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

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

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

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

К такому сертификату предъявляются следующие требования:
- имя сертификата (Common name) должно совпадать с именем публикуемого Web-сервера прикладной системы. Например: pif.nikoil.ru;
- поле расширения сертификата «Использование ключа» должно содержать следующее назначение: «Аутентификация Сервера».

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

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

2.3 Проверка использования российских алгоритмов в браузерах Internet Explorer/Microsoft Edge

Для проверки использования российских алгоритмов при доступе к веб-странице с помощью браузеров Internet Explorer и Microsoft Edge выполните следующие действия:

1) Откройте веб-страницу в браузере Internet Explorer/Microsoft Edge. При посещении веб-страницы обратите внимание, используется ли протокол соединения «https».

2) Нажмите на значок «замка» (см. рис. 5, рис. 6).

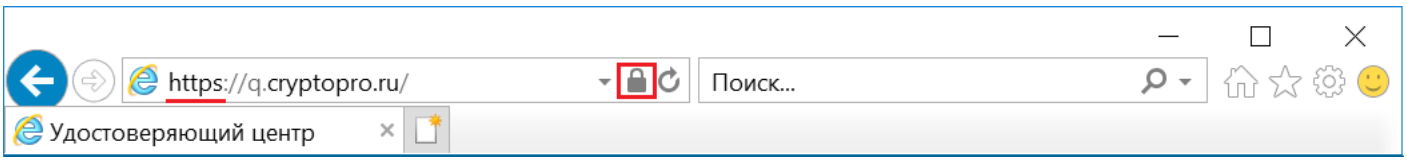


Рисунок 5. Адресная строка Internet Explorer

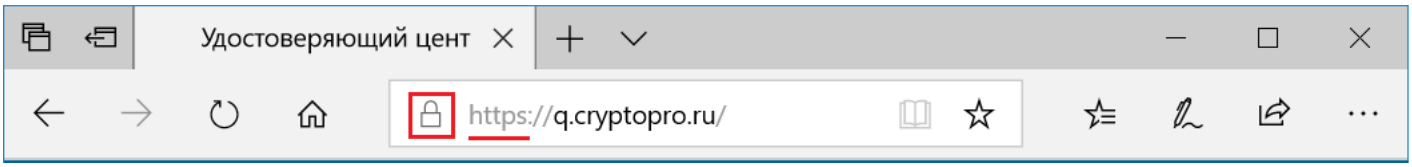


Рисунок 6. Адресная строка Microsoft Edge

3) Откроется окно «Идентификация веб-сайта» (см. рис. 7). В окне нажмите на кнопку **Просмотр сертификатов** (**Просмотреть сертификат**).

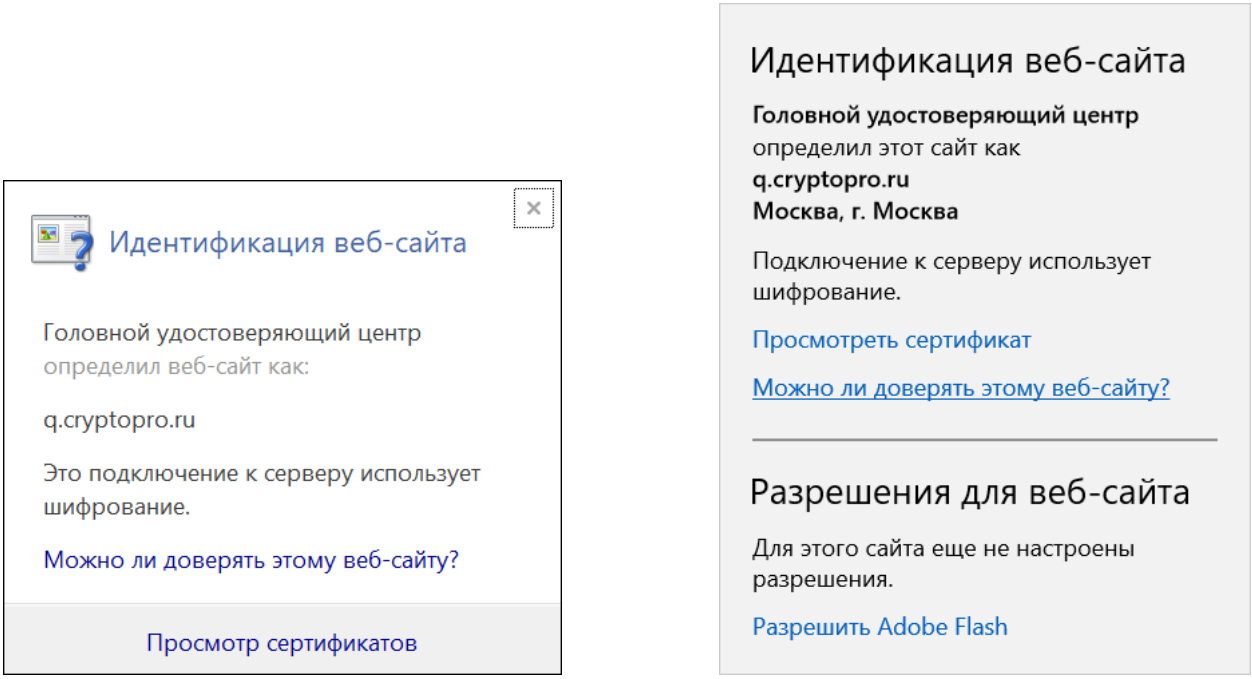


Рисунок 7. Окно идентификации веб-сайта в браузерах Internet Explorer и Microsoft Edge

4) Откроется окно со сведениями о сертификате веб-сервера, включая информацию об используемых криптографических алгоритмах (см. рис. 8).

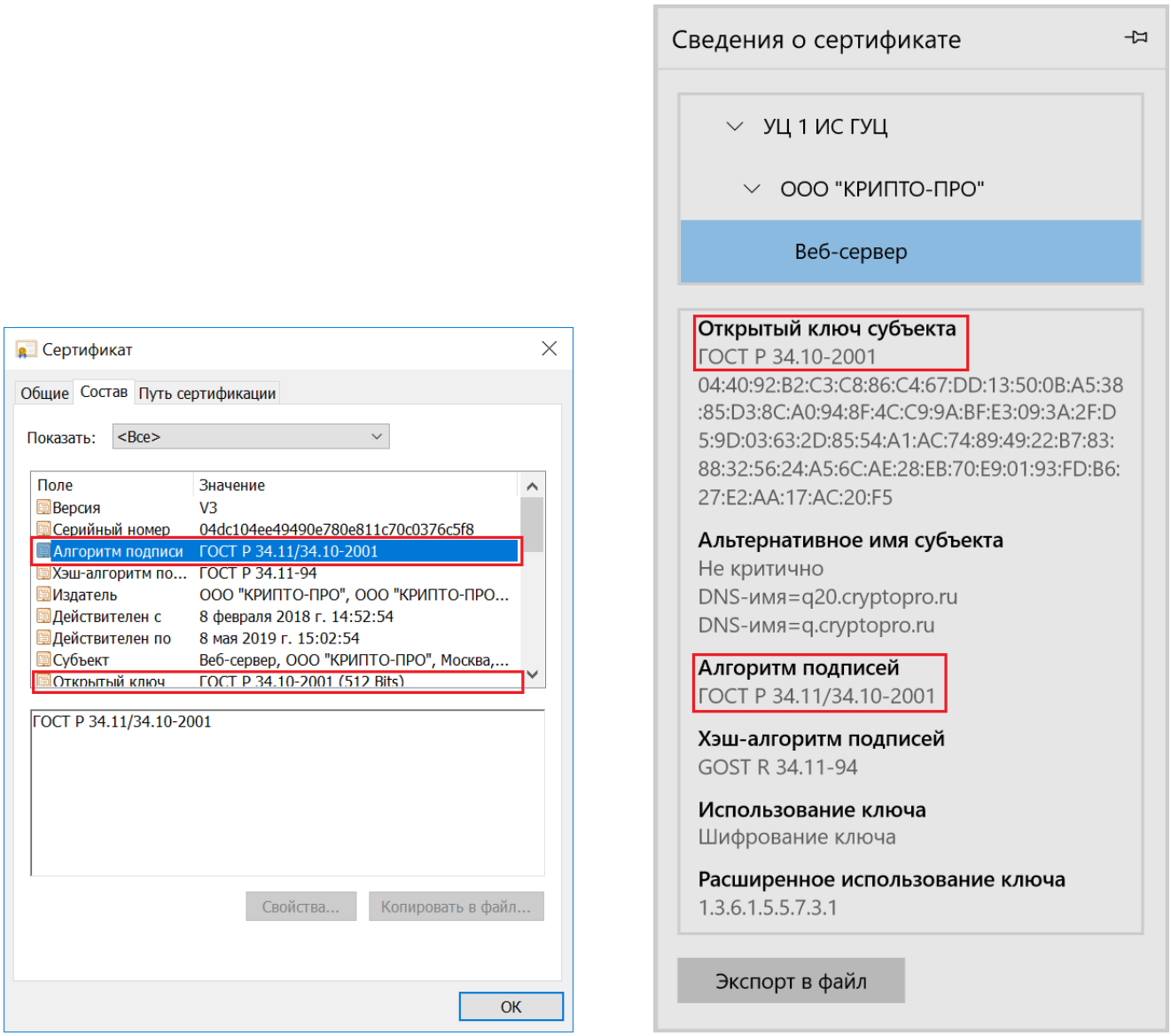


Рисунок 8. Окно со сведениями о сертификате веб-сервера в браузерах Internet Explorer и Microsoft Edge

3 Разбор конфликтных ситуаций, связанных с применением ЭП

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

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

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

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

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

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

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

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

3.1 Порядок разбора конфликтной ситуации

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

1) предъявления претензии одной стороны другой;
2) формирования комиссии;
3) разбора конфликтной ситуации;
4) принятие мер по урегулированию конфликта.

Разбор конфликтной ситуации проводится с использованием программного обеспечения СКЗИ КриптоПро CSP версии 5.0 КС1 для электронного документа, авторство или содержание которого оспаривается.

Проверка подписанного электронного документа включает в себя выполнение следующих действий:

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

При проверке ЭП 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 ключа ЭП не влияют на определение авторства документа. В таком случае можно сделать предположение о несоблюдении пользователем Регламента (Договора) в части сроков действия ключей, сертификатов или некорректного использования сертификата в прикладном ПО.

3.2 Случаи невозможности проверки значения ЭП

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

4 Нештатные ситуации при эксплуатации СКЗИ

В табл. 2 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
1	Эвакуация, угроза нападения, взрыва, стихийные бедствия, аварии общего характера в Центре управления ключевой системой.	Остановить все ЭВМ. Персонал, имеющий доступ к ключам, обязан сдать все имеющиеся у него в наличии ключевые носители администратору безопасности. Администратор безопасности упаковывает все ключевые носители, регистрационные карточки сертификатов открытых ключей пользователей, сертификаты ключей проверки ЭП пользователей в опечатываемый контейнер, который выносит в безопасное помещение или здание. Опечатанный контейнер должен находиться под охраной до окончания действия нештатной ситуации и восстановления нормальной работы аппаратных и программных средств СКЗИ. Администратор безопасности оповещает по телефонным каналам общего пользования всех пользователей о приостановке работы системы. В случае наступления события, повлекшего за собой долговременный выход из строя аппаратных средств СКЗИ, администратор безопасности уничтожает всю ключевую информацию с носителей, находящихся в контейнере.
2	Компрометация одного из личных ключевых носителей.	Порядок действий при компрометации ключей описан в разделе 3 документа ЖТЯИ.00101-01 95 01. Правила пользования.
3	Выход из строя первого личного ключевого носителя.	Необходимо сообщить по телефону в УЦ о факте выхода из строя личного ключевого носителя и обеспечить его доставку в УЦ для выяснения причин выхода из строя. Для работы используется второй личный ключевой носитель.
4	Выход из строя второго личного ключевого носителя (при условии, что первый тоже вышел из строя).	Пользователь, у которого вышли из строя оба личных ключевых носителя, является в УЦ для повторной регистрации (без изменения данных регистрации).
5	Отказы и сбои в работе аппаратной части АРМ со встроенной СКЗИ.	При отказах и сбоях в работе аппаратной части АРМ со встроенным СКЗИ необходимо остановить работу, по возможности локализовать неисправность и в дальнейшем произвести ремонт в установленном порядке и, при необходимости, переустановку СКЗИ.
6	Отказы и сбои в работе средств защиты от НСД.	При отказах и сбоях в работе средств защиты от НСД, администратор безопасности, должен восстановить работоспособность средств НСД. При необходимости переустановить программно-аппаратные средства НСД.
7	Утеря личного ключевого носителя.	Утеря личного ключевого носителя приводит к компрометации хранящегося в нем ключа. Порядок действий при компрометации ключей описан в разделе 3 документа ЖТЯИ.00101-01 95 01. Правила пользования.

8	Отказы и сбои в работе программных средств вследствие не выявленных ранее ошибок в программном обеспечении.	При отказах и сбоях в работе программных средств, вследствие не выявленных ранее ошибок в программном обеспечении, необходимо остановить работу, локализовать по возможности причину отказов и сбоев и вызвать разработчика данного ПО или его представителя для устранения причин, вызывающих отказы и сбои.
9	Отказы в работе программных средств вследствие случайного или умышленного их повреждения.	При отказах в работе программных средств, вследствие случайного или умышленного их повреждения, ответственное за безопасность функционирования программных и аппаратных средств лицо обязано произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы программных средств в установленном порядке.
10	Отказы в работе программных средств вследствие ошибок оператора.	При отказах в работе программных средств, вследствие ошибок оператора, оператор сообщает о данном факте лицу, ответственному за безопасность функционирования программных и аппаратных средств. Ответственный за безопасность функционирования программных и аппаратных средств дает соответствующие указания обслуживающему персоналу по восстановлению правильной работы программных средств в установленном порядке.

5 Требования по защите от НСД

5.1 Общие требования по организации работ по защите от НСД

Защита аппаратного и программного обеспечения от НСД при установке и использовании СКЗИ КриптоПро CSP версии 5.0 KC1 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 СКЗИ.

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.

5.2 Требования по размещению технических средств с установленным СКЗИ

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

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

Размещение СКЗИ КриптоПро CSP версии 5.0 KC1 в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.

В целях защиты открытой конфиденциальной информации от утечки по техническим каналам, в том числе по каналам связи, от объектов информатизации и СКЗИ, ввод в действие и эксплуатация указанных объектов и СКЗИ должна осуществляться в соответствии с действующими в Российской Федерации требованиями по защите информации от утечки по техническим каналам, в том числе по каналу связи (например, СТР-К).

Необходимость и достаточность мер, в том числе по каналу связи, должна оцениваться порядком, предусмотренным упомянутыми руководящими документами, с учетом целевых установок предполагаемого нарушителя и угроз безопасности информации, определяемых моделью угроз и нарушителя. При этом, если объекты аттестованы на соответствие установленным требованиям по защите информации без учета оценки канала связи, при подключении таких средств к каналам связи, выходящим за пределы контролируемой территории, необходимо использовать любое

из следующих средств:

- Волоконно-оптические линии связи;
- Оптические развязывающие устройства, устанавливаемые в тракт передачи информации для создания оптоволоконного фрагмента сети;
- Сертифицированные СКЗИ для передачи информации соответствующего уровня конфиденциальности.

Для мобильных программно-аппаратных платформ для обеспечения защиты информации по классу КС от утечки по каналу линейной передачи достаточно, чтобы канал связи был реализован в виде радиоканала GSM, либо GPRS, либо 3G/4G, либо Wi-Fi, либо другого канала мобильной и беспроводной связи, работающего в диапазоне частот несущей выше 800 МГц с цифровой модуляцией штатного информационного сигнала.

5.3 Требования по установке СКЗИ, общесистемного и специального ПО на ПЭВМ

ПЭВМ, на которых используется СКЗИ, должны быть допущены для обработки конфиденциальной информации по действующим в Российской Федерации требованиям по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К), с учетом модели угроз в информационной системе заказчика, которым должно противостоять СКЗИ КриптоПро CSP версии 5.0 КС1.

Инсталляция СКЗИ КриптоПро CSP версии 5.0 КС1 на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.

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

При установке программного обеспечения СКЗИ следует:

- На технических средствах, предназначенных для работы с СКЗИ, использовать только лицензионное программное обеспечение фирм-изготовителей.
- При установке ПО СКЗИ на ПЭВМ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ и совместно поставляемых с СКЗИ компонент СФ.
- 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.

5.4 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.);

- необходимо использовать фильтры паролей в соответствии со следующими правилами:
  - длина пароля должна быть не менее 8 символов;
  - в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
  - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);
  - при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
  - личный пароль пользователь не имеет права сообщать никому;
  - периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев.
- пароли для аутентификации пользователей на носителях, работающих в режиме активного вычислителя с защитой канала между носителем и СКЗИ по протоколу SESPAKE, должны удовлетворять следующим требованиям:
  - для выработки общего ключа с аутентификацией на основе пароля при использовании кривых с 512-битовым порядком группы точек:
    - пароль должен состоять из букв английского алфавита и верхнем и нижнем регистрах, цифр и спецзнаков;
    - минимальная длина пароля — 4 символа;
    - периодичность смены пароля — не реже 1 раза в полгода.
  - для выработки общего ключа с аутентификацией на основе пароля при использовании кривых с 256-битовым порядком группы точек:
    - пароль должен состоять из букв английского алфавита и верхнем и нижнем регистрах, цифр и спецзнаков;
    - минимальная длина пароля — 10 символов;
    - периодичность смены пароля — не реже 1 раза в 56 дней.
- политика назначения и смены паролей должна удовлетворять следующим требованиям: после трех неверных попыток ввода пароля пользователем при входе в ОС система должна блокироваться на 1 час (с обеспечением возможности разблокировки учетной записи при обращении пользователя к администратору безопасности);
- указанная политика обязательна для всех учетных записей, зарегистрированных в ОС;
- средствами BIOS должна быть исключена возможность работы на ПЭВМ с СКЗИ, если во время её начальной загрузки не проходят встроенные тесты;
- в качестве меры по усилению защиты от НСД следует запретить сохранение паролей, используемых в работе СКЗИ. Для этого предпочтительнее воспользоваться групповыми политиками. Инструкции по настройке групповых политик см. в соответствующем используемой программно-аппаратной платформе дополнении к Руководству администратора безопасности.

При эксплуатации СКЗИ **ЗАПРЕЩАЕТСЯ**:

- оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации (за исключением случаев, предусмотренных данными правилами);
- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;
- записывать на ключевые носители постороннюю информацию;
- вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя;
- подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией;
- работать на компьютере, если во время его начальной загрузки не проходит встроенный тест ОЗУ, предусмотренный в ПЭВМ;
- изменять настройки, установленные программой установки СКЗИ или администратором;
- использовать синхропосылки, вырабатываемые не средствами СКЗИ;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации, подлежащей уничтожению в соответствии с п. 3.9.3 документа ЖТЯИ.00101-01 95 01. Правила пользования, средствами СКЗИ;
- осуществлять несанкционированное вскрытие системных блоков ПЭВМ.

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

- недопустимо использовать нестандартные, измененные или отладочные версии ОС;
- необходимо исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой (например, путем опечатывания устройства загрузки и последующего контроля целостности печатей);
- необходимо исключить возможность удаленного управления, администрирования и модификации ОС и её настроек;
- на ПЭВМ должна быть установлена только одна ОС (в случае использования виртуальной инфраструктуры допускается использование одной хостовой и неограниченного количества гостевых ОС);
- правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности;
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);
- режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права;
- необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
  - системный реестр;
  - файлы и каталоги;
  - временные файлы;
  - журналы системы;
  - файлы подкачки;
  - кэшируемая информация (пароли и т.п.);
  - отладочная информация.

Кроме вышеперечисленного, необходимо организовать стирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям (см. раздел 3 документа ЖТЯИ.00101-01 95 01. Правила пользования).

- должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;
- необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;
- в случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вредоносного ПО, 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.

5.5 Требования по обеспечению физической безопасности сервера

Следует исключить возможность доступа неавторизованного персонала к консоли, системе питания и дополнительным устройствам, подключенным к защищаемому серверу путем установки оборудования в специально выделенное и запираемое помещение (аппаратную или серверную комнату).

Доступ персонала в серверную комнату должен быть регламентирован внутренним распорядком эксплуатирующей

организации и должностными инструкциями.

Для исключения сбоев компьютера, вызванных отключением электропитания, необходимо обеспечить электропитание сервера от источника бесперебойного питания достаточной мощности. Как минимум, мощности батарей источника бесперебойного питания должно хватать на время достаточное для корректного автоматического завершения работы сервера.

5.6 Требования по организации процедуры резервного копирования и хранения резервных копий

При определении регламента резервного копирования и хранения резервных копий следует обеспечить ответственное хранение резервных копий в запираемых сейфах (шкафах) и определить процедуру выдачи резервных копий ответственному персоналу и уничтожения вышедших из употребления носителей (лент, однократно записываемых дисков и пр.).

Стандартными мерами по организации ответственного хранения носителей являются:

- маркировка носителей;
- составление описи хранимых носителей с указанием серийных (инвентарных) номеров, дат записи носителей, фамилией сотрудника, создавшего копию для каждого шкафа(сейфа);
- периодическая сверка описи и содержимого сейфов (шкафов);
- организация ответственного хранения и выдачи ключей от сейфов (шкафов);
- возможное опечатывание (опломбирование) сейфов(шкафов).
- уничтожение вышедших из употребления носителей должно производиться комиссией с составлением акта об уничтожении.

5.7 Требования по подключению СКЗИ для работы по общедоступным каналам передачи данных

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.

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

- Порядок подключения СКЗИ к каналам связи.
- Выделено лицо, ответственное за безопасность работы по общедоступным каналам.
- Разработан типовой регламент защищенной связи, включающий:
  - политику безопасности защищенной связи.
  - допустимый состав прикладных программных средств, для которого должно быть исследовано и обосновано отсутствие негативного влияния на СКЗИ по каналу передачи данных.
  - перечень допустимых сетевых протоколов.
  - защиту сетевых соединений (перечень допустимых сетевых экранов).
  - систему и средства антивирусной защиты.

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

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

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

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.

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

Программно-аппаратные средства защиты от НСД предназначены для организации защиты компьютера от входа посторонних пользователей. Под посторонними пользователями понимаются все лица, не зарегистрированные в системе как пользователи данного компьютера.

Необходимо использовать средство защиты от несанкционированного доступа, сертифицированное ФСБ России. Поставка осуществляется по согласованию с пользователем

Программно-аппаратные средства защиты от НСД обеспечивают:

- регистрацию пользователей компьютера и назначение им персональных идентификаторов и паролей на вход в систему;
- идентификацию и аутентификацию пользователя при загрузке компьютера;
- ведение системного журнала, в котором производится регистрация событий, имеющих отношение к безопасности системы;
- контроль целостности программного и аппаратного обеспечения защищаемого компьютера;
- защиту от несанкционированной загрузки операционной системы со съемных носителей;
- наличие в составе аппаратного датчика случайных чисел (ДСЧ).

Установка и настройка программно-аппаратного средства защиты от НСД на АРМ пользователя должна производиться в соответствии с эксплуатационной документацией. Перед эксплуатацией программно-аппаратного средства защиты от НСД в составе АРМ пользователя необходимо ознакомиться с комплектом документации на данное средство и принять рекомендуемые в документации защитные организационные меры.

Настройка программно-аппаратного средства защиты от НСД 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.

6 Требования по криптографической защите

Должны выполняться следующие требования по криптографической защите:

1) Допустимо использование только лицензионного системного программного обеспечения.

2) Настройки операционных систем для работы с СКЗИ должны производиться в соответствии с документами:

- ЖТЯИ.00101-01 91 02 Руководство администратора безопасности. Windows
- ЖТЯИ.00101-01 91 03 Руководство администратора безопасности. Linux
- ЖТЯИ.00101-01 91 04 Руководство администратора безопасности. FreeBSD
- ЖТЯИ.00101-01 91 05 Руководство администратора безопасности. Solaris
- ЖТЯИ.00101-01 91 06 Руководство администратора безопасности. AIX
- ЖТЯИ.00101-01 91 07 Руководство администратора безопасности. Mac OS
- ЖТЯИ.00101-01 91 08 Руководство администратора безопасности. iOS
- ЖТЯИ.00101-01 91 09 Руководство администратора безопасности. Виртуальные среды
- ЖТЯИ.00101-01 91 10 Руководство администратора безопасности. Sailfish
- ЖТЯИ.00101-01 91 11 Руководство администратора безопасности. Android

3) При установке ПО СКЗИ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ и совместно поставляемых с СКЗИ компонент СФ. После завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО СКЗИ, а также его окружения.

4) Контролем целостности должны быть охвачены файлы, указанные в разделах «Требования по криптографической защите» документов ЖТЯИ.00101-01 91 02, ЖТЯИ.00101-01 91 03, ЖТЯИ.00101-01 91 04, ЖТЯИ.00101-01 91 05, ЖТЯИ.00101-01 91 06, ЖТЯИ.00101-01 91 07, ЖТЯИ.00101-01 91 08, ЖТЯИ.00101-01 91 09, ЖТЯИ.00101-01 91 10, ЖТЯИ.00101-01 91 11

5) Если проверка целостности компонентов СКЗИ завершается ошибкой, администратор безопасности должен выявить причину и обстоятельства нарушения целостности СКЗИ и переустановить СКЗИ в соответствии с инструкцией по установке, описанной в руководстве администратора безопасности для используемой программно-аппаратной платформы.

6) Необходимо исключить из программного обеспечения ПЭВМ с установленным СКЗИ средства отладки.

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

8) Ключевая информация является конфиденциальной.

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

10) Пароль, используемый для аутентификации пользователей, должен удовлетворять требованиям разд. 5.4.

11) Периодичность тестового контроля криптографических функций — 10 минут.

12) Ежесуточная перезагрузка ПЭВМ.

13) Периодичность останова ПЭВМ с обязательной проверкой системы охлаждения процессорного блока ПЭВМ — 1 месяц.

14) Запрещается использовать режим простой замены (ECB) ГОСТ 28147-89 для шифрования информации, кроме ключевой.

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

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

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

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

19) Запрещается использование беспроводных клавиатур и компьютерных мышей.

7 Требования по встраиванию и использованию ПО СКЗИ

Встраивание СКЗИ в защищаемые информационные системы должно производиться в соответствии с Положением ПКЗ-2005 [20]. Встраивание должны проводить организации, имеющие лицензию на право проведения таких работ.

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

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

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

1) Через интерфейс функций CryptoAPI 2.0, что позволяет применять весь инструментарий фирмы Microsoft. Для этих целей разработчики могут воспользоваться программной документацией, содержащейся в MSDN (Microsoft Developer Network), а также поставляемым тестовым ПО; на Unix-платформах (Linux, FreeBSD, Solaris) через интерфейс библиотеки capilite.dll, являющейся подмножеством интерфейса CryptoAPI 2.0. Для этих целей в комплект поставки включается документ ЖТЯИ.00101-01 96 01. Руководство программиста.

2) Путем непосредственного вызова функций СКЗИ после загрузки модуля с использованием функции LoadLibrary. Для этих целей в комплект поставки включается документ ЖТЯИ.00101-01 96 01. Руководство программиста, описывающий состав функций и тестовое ПО.

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

При встраивании СКЗИ в прикладное программное обеспечение должны выполняться требования документа ЖТЯИ.00101-01 96 01. Руководство программиста.

Правила встраивания и использования СКЗИ

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

1) При использовании открытого ключа или ключа проверки ЭП должны быть обеспечены его авторизация, достоверность, целостность и идентичность. Это может быть реализовано:

- путем заверения открытого ключа или ключа проверки ЭП доверенной стороной (например, в случае использования сертификатов открытых ключей);
- путем доверенного распространения и хранения открытых ключей и ключей проверки ЭП в виде справочников.

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

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

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

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

Литература

[1] ЖТЯИ.00101-01 30 01. КриптоПро CSP. Формуляр.

[2] ЖТЯИ.00101-01 90 01. КриптоПро CSP. Описание реализации.

[3] ЖТЯИ.00101-01 95 01. КриптоПро CSP. Правила пользования.

[4] ЖТЯИ.00101-01 91 02. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows.

[5] ЖТЯИ.00101-01 91 03. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux.

[6] ЖТЯИ.00101-01 91 04. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС FreeBSD.

[7] ЖТЯИ.00101-01 91 05. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Solaris.

[8] ЖТЯИ.00101-01 91 06. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС AIX.

[9] ЖТЯИ.00101-01 91 07. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Mac OS X.

[10] ЖТЯИ.00101-01 91 08. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС iOS.

[11] ЖТЯИ.00101-01 91 09. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ в виртуальных средах.

[12] ЖТЯИ.00101-01 91 10. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Sailfish.

[13] ЖТЯИ.00101-01 91 11. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Android.

[14] ЖТЯИ.00101-01 91 12. КриптоПро CSP. Руководство администратора безопасности. Использование JavaCSP и JavaTLS.

[15] ЖТЯИ.00101-01 92 01. КриптоПро CSP. Инструкция по использованию СКЗИ под управлением ОС Windows.

[16] ЖТЯИ.00101-01 94 01. КриптоПро CSP. АРМ выработки внешней гаммы.

[17] ЖТЯИ.00101-01 96 01. КриптоПро CSP. Руководство программиста.

[18] RFC 2246 The TLS Protocol Version 1.0. URL: https://www.ietf.org/rfc/rfc2246.txt.

[19] Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26). Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS). URL: https://tc26.ru/standarts/metodicheskie-rekomendatsii/ispolzovanie-naborov-algoritmov-shifrovaniya-na-osnove-gost-28147-89-dlya-protokola-bezopasnosti-transportnogo-urovnya-tls.html.

[20] Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)». URL: http://base.garant.ru/187947/.

Лист регистрации изменений

Лист регистрации изменений									
№ п/п	Номера листов (страниц)				Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					