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

Средство Криптографической Защиты Информации

КриптоПро JCP

Версия 2.0

Руководство администратора безопасности

Общая часть

ЖТЯИ.00091-01 90 01

Листов 84

2016 г.

Оглавление

1. Введение

Настоящее руководство содержит общее описание средства криптографической защиты информации (СКЗИ) «КриптоПро JCP» версия 2.0, его состав, ключевую систему, рекомендации по размещению технических средств, использующих СКЗИ, рекомендации по проверке целостности установленного ПО СКЗИ, по использованию СКЗИ в различных автоматизированных системах и средствах вычислительной техники.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро JCP» версия 2.0, должны разрабатываться с учетом требований настоящего Руководства.

Криптопровайдер «КриптоПро JCP» версия 2.0 является средством криптографической защиты информации (СКЗИ «КриптоПро JCP» версия 2.0), реализующим российские криптографические алгоритмы и функционирующим под управлением виртуальной машины Java 2 Runtime Environment версии 1.6 и выше.

2. Список сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
IETF	Internet Engineering Task Force
ITU-T	Международный комитет по телекоммуникациям (International Telecommunication Union)
АС	Автоматизированная система
АРМ	Автоматизированное рабочее место
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск
КП	Конечный пользователь
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
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.
СФК	Среда функционирования комплекса
ЦС	Центр Сертификации УЦ
УЦ	Удостоверяющий Центр
ЦС	Центр Сертификации
ЦР	Центр Регистрации УЦ
ЭД	Электронный документ
ЭП	Электронная подпись

3. Основные термины и положения

Автоматизированная информационная система

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

Автоматизированная система

Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [ГОСТ 34003].

Авторство информации

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

Актуальность информации

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

Администратор безопасности

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

Основные направления деятельности администратора безопасности:

1. контроль целостности программного обеспечения;
2. управление ключевой системой: хранение, ввод в действие и смена ключей пользователей, генерация ключей электронной подписи и ключей проверки подписи пользователей;
3. управление доступом пользователей системы к программному обеспечению и данным, включая установку и периодическую смену паролей, управление средствами защиты коммуникаций, передаваемых, хранимых и обрабатываемых данных.

Администратор защиты

Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации [ГТК Термины].

Аутентификация

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

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 [Бияшев].

Безопасность

1. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз [РФ.Безопасность].
2. Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба [ГОСТ 1].

Безопасность информации (информационная безопасность)

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

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

Блокирование информации

Прекращение или затруднение доступа законных пользователей к информации [ГТК защита].

Верификация

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

Владелец информации

1. Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации [ГОСТ 50922].
2. Субъект информационных отношений, обладающий правом владения, распоряжения и пользованием информационным ресурсом по договору с собственником информации [Терминология].

Владелец информации, информационной системы

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

Государственная тайна

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

Гриф конфиденциальности

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

Гриф секретности

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

Документ

1. Документированная информация, снабженная определенными реквизитами [РФ.Защита].
2. Материальный объект с информацией, закрепленной созданным человеком способом для ее передачи во времени и пространстве [ГОСТ 16487].

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 [РФ.Защита].

Документ в электронной форме (Электронный документ)

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

ЭД представляет собой задокументированную совокупность данных, зафиксированных на материальном носителе (магнитном или бумажном) с реквизитами, позволяющими идентифицировать эту информацию и авторов документа. Идентификация ЭД обеспечивается средствами защиты 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

1. Получение субъектом возможности ознакомления с информацией, в том числе с помощью технических средств [ГОСТ 50922].
2. Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации [ГТК Термины].

Доступность информации

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

Заверение (нотаризация)

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

Защита информации

1. Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [ГОСТ 50922].
2. Комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации [Лицензирование].

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 [ГТК Классификация].

Защищенное средство вычислительной техники (защищенная автоматизированная система)

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

Идентификация

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

Имитозащита

Защита системы шифрованной связи от навязывания ложных данных [ГОСТ 28147].

Имитовставка

Отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты [ГОСТ 28147].

Ключ (криптографический ключ)

Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований [ГОСТ 28147].

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) ключа ЭП.
5. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
6. Нарушение печати на сейфе с ключевыми носителями.
7. Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)

Различают два вида компрометации ключа ЭП: явную и неявную. Первые четыре события должны трактоваться как явная компрометация ключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

Конфиденциальность информации

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

Конфиденциальная информация

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

Контроль доступа (управление доступом)

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

Криптографическая защита

Защита данных при помощи криптографического преобразования данных [ГОСТ 28147].

Криптопровайдер

Криптопровайдер - библиотека классов реализованная по стандарту JCA. Может реализовывать функции шифрования, вычисления имитовставки, хэширования, формирования и проверки подписи, генерирования пользовательских ключей. Может обеспечивать работу с сессионными ключами шифрования (генерация, экспорт/импорт в защищенном виде), ключами ЭП ключами проверки ЭП, закрытыми и открытыми ключами обмена, ввод ключей с ключевых носителей, защищённое хранение и уничтожение ключей.

Криптографическое преобразование

Преобразование данных при помощи шифрования и (или) выработки имитовставки [ГОСТ 28147].

Лицензирование в области защиты информации

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

Мероприятия по защите информации

Совокупность действий по разработке и/или практическому применению способов и средств защиты информации [ГОСТ 50922].

Мероприятия по контролю эффективности защиты информации

Совокупность действий по разработке и/или практическому применению способов и средств контроля эффективности защиты информации [ГОСТ 50922].

Метка конфиденциальности

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

Нарушитель безопасности информации

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

Нарушитель правил разграничения доступа

Субъект доступа, осуществляющий несанкционированный доступ к информации [ГТК Термины].

Некорректный электронный документ

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

Непреднамеренное воздействие на информацию

Ошибка пользователя информацией, сбой технических и программных средств информационных систем, а также природное явление или иное нецеленаправленное на изменение информации воздействие, связанное с функционированием технических средств, систем или с деятельностью людей, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [ГОСТ 50922].

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 [ГОСТ 50922].

Несанкционированный доступ к информации (НСД)

1. Получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации [ГОСТ 50922]
2. Доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или автоматизированной системы (АС) [ГТК Термины] [ГТК НСД].

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 [ГОСТ 50922].

Объект доступа

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

Объект защиты

1. Информация или носитель информации, или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации [ГОСТ 50922].
2. Информация, технические средства и технология ее обработки, в отношении которых необходимо обеспечить безопасность информации [ГТК защита].

Обработка информации

Передача, прием, хранение, преобразование и отображение информации.

Организация защиты информации

Содержание и порядок действий по обеспечению защиты информации [ГОСТ 50922].

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 зашифрования, позволяет определить автора подписи и достоверность электронного документа, но не позволяет вычислить закрытый ключ. Открытый ключ считается принадлежащим пользователю, если он был зарегистрирован (сертифицирован) установленным порядком.

Пароль

1. Идентификатор субъекта доступа, который является его (субъекта) секретом [ГТК Термины].
2. Секретная информация аутентификации, обычно представляющая собой строку знаков, которой должен обладать пользователь для доступа к защищенным данным.

Плановая смена ключей

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

Побочные электромагнитные излучения и наводки

1. Электромагнитные излучения технических средств обработки информации, не предназначенные для передачи, приема или преднамеренного искажения информации, а также наводки от технических средств в окружающих предметах [ГТК защита].
2. Нежелательные излучения и наводки, проявляющиеся в виде побочных, внеполосных, шумовых и наводимых сигналов, потенциально образующих неконтролируемые каналы утечки конфиденциальной информации [Халянин].

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 [Терминология].

Пользователи

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

Пользователь (потребитель) информации

1. Субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею [РФ.Защита].
2. Субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением [ГОСТ 50922].

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 [ГОСТ 50922].

Правила разграничения доступа (ПРД)

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

Право доступа к защищаемой информации; право

Совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации [ГОСТ 50922].

Проверка электронной подписи документа

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

Разглашение информации

Несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к этой информации [ГОСТ 50922].

Расшифрование данных

Процесс преобразования зашифрованных данных в открытые данные при помощи шифра [ГОСТ 28147].

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 [Халянин].

Санкционированный доступ к информации

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

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 [ГТК Термины].

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

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

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

Сертификат соответствия

Документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям [РФ.Сертификация].

Секретный (закрытый) ключ

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

Система защиты информации

Совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации [ГОСТ 50922].

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 [ГТК Термины].

Служебная и коммерческая тайна

1. Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного

доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами [РФ.ГК].

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

Собственник информации

1. Субъект информационных отношений, обладающий юридическим правом владения, распоряжения и пользования информационным ресурсом. Юридическое право владения, распоряжения и пользования информационным ресурсом принадлежит лицам, получившим этот информационный ресурс по наследству. Авторам открытий, изобретений, научно-технических разработок, рационализаторских предложений и т.д. принадлежит право владения, распоряжения и пользования информацией, источником которой они являются [Терминология].
2. Субъект, в полном объеме реализующий полномочия владения, пользования и распоряжения информацией в соответствии с законодательными актами [ГОСТ 50922].
3. Юридическое или физическое лицо, владеющее информацией в соответствии с Законом о собственности [ГТК защита].

Способ защиты информации

Порядок и правила применения определенных принципов и средств защиты информации [ГОСТ 50922].

Способы несанкционированного доступа

1. Приемы и порядок действий с целью получения (добывания) охраняемых сведений незаконным путем. К ним в том числе относятся:
    - инициативное сотрудничество (предательство, измена).
    - склонение (принуждение, побуждение) к сотрудничеству (подкуп, шантаж);
    - подслушивание переговоров;
    - незаконное ознакомление;
    - хищение;
    - подделка (модификация);
    - уничтожение (порча, разрушение);
    - незаконное подключение к системам и линиям связи и передачи информации;
    - перехват акустических и электромагнитных сигналов;
    - визуальное наблюдение;
    - фотографирование;
    - сбор и анализ документов, публикаций и промышленных отходов [Халянин].
2. К основным способам НСД относятся:
    - непосредственное обращение к объектам доступа;
    - создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
3. модификация средств защиты, позволяющая осуществить НСД;
4. внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД [ГТК НСД].

Средства вычислительной техники

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

Средство защиты информации

Техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации [ГОСТ 50922].

Средство защиты от несанкционированного доступа

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

Средство криптографической защиты информации

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

Субъект доступа

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

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 [Терминология].

Техническое средство обработки информации

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

Угроза безопасности

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

Удостоверяющий центр

Центр управления ключами проверки ЭП в соответствии с рекомендациями X509 в части использования сертификатов ключей проверки ЭП.

Уничтожение информации

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

Управление ключами

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

Утечка информации

1. Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведкой [ГОСТ 50922].
2. Неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация доверена [Халянин].

Функция хэширования

Заключается в сопоставлении произвольного набора данных в виде последовательности двоичных символов и его образа фиксированной небольшой длины, что позволяет использовать эту функцию в процедурах электронной подписи для сокращения времени подписи и проверки подписи. Эффект сокращения времени достигается за счет вычисления подписи только под образом подписываемого набора данных [ГОСТ 341094].

Целостность информации

1. Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения) [ГТК Термины].
2. Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Цель защиты информации

Заранее намеченный результат защиты информации.

1. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию [ГОСТ 50922].
2. Целями защиты являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение угроз безопасности личности, общества, государства; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах, сохранение государственной тайны конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения [РФ.Защита].

Шифр

Совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей [ГОСТ 28147].

Шифрование

Процесс зашифрования или расшифрования [ГОСТ 28147].

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

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

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

Шифрование документов (текстов)

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

Шифровальные средства

Средства криптографической защиты информации:

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

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

Проверка электронной подписи под блоком открытой информации производится с помощью криптографического преобразования и ключа проверки электронной подписи, соответствующего ключу электронной подписи, участвовавшего в процессе установки 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 электронной подписи вместо обычной связи между печатью или рукописной подписью и листом бумаги выступает сложная математическая зависимость между электронным документом, ключом ЭП и ключом 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.

4. Основные технические данные и характеристики СКЗИ

СКЗИ «КриптоПро JCP» версия 2.0 является криптопровайдером Java и предназначено для защиты конфиденциальной информации.

СКЗИ «КриптоПро JCP» версия 2.0 совместимо КриптоПро CSP по выполняемым криптографическим функциям и ключам (см. «Совместимость с продуктами КриптоПро»).

Средствами СКЗИ «КриптоПро JCP» версия 2.0 **не допускается** защищать информацию, составляющую государственную тайну.

СКЗИ «КриптоПро JCP» версия 2.0 при условии выполнения настоящих Правил обеспечивает криптографическую защиту конфиденциальной информации от внешнего нарушителя, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки.

СКЗИ предназначено для защиты информации, передаваемой по каналам связи, и обеспечивает:

- авторизацию электронных документов на базе электронной подписи;
- аутентификацию сторон при передаче электронных документов на базе протоколов TLS;
- защищенную парно-выборочную связь для обмена конфиденциальной информацией.

4.1. Функции защиты информации СКЗИ

СКЗИ ЖТЯИ.00091-01 обеспечивает выполнение следующих функций защиты информации:

- авторизация и обеспечение юридической значимости электронных документов при обмене ими между пользователями посредством использования процедур формирования и проверки (с использованием сертификатов стандарта X.509 Удостоверяющего центра) электронной подписи в соответствии с отечественными стандартами (RFC 4357):

ГОСТ Р 34.10-2001. *"Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".*

ГОСТ Р 34.10-2012. *"Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".*

ГОСТ Р 34.11-94. *"Информационная технология. Криптографическая защита информации. Функция хэширования"*.

ГОСТ Р 34.11-2012. *"Информационная технология. Криптографическая защита информации. Функция хэширования"*.

- обеспечение конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с отечественным стандартом:

ГОСТ 28147-89 *"Системы обработки информации. Защита криптографическая"*;

- контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированного изменения или от нарушения правильности функционирования;
- управления ключевыми элементами системы в соответствии с регламентом;
- обеспечение аутентификации связывающихся сторон, конфиденциальности и целостности пересылаемой информации с использованием сертификатов стандарта X.509;
- установление аутентичного защищенного соединения с использованием протокола TLS;
- обеспечение конфиденциальности и контроля целостности и авторизация файлов и информационных сообщений;
- обеспечение аутентификации, аутентификация пользователя в домене Windows.

Дополнительные алгоритмы поддержки ключевых систем, параметры алгоритмов, форматы сертификатов, поддерживаемые в СКЗИ, определены в документах RFC 4357, RFC 4490, RFC 4491.

4.2.Механизмы защиты информации

- Конфиденциальность информации при хранении (на дисках, в базе данных) и передаче в сети связи обеспечивается использованием функций шифрования.

- Идентификация и авторство. При сетевом взаимодействии (установлении сеанса связи) обеспечивается функциями ЭП при использовании их в процессе аутентификации (например, в соответствии с рекомендациями X.509). При электронном документообороте обеспечивается использованием функций ЭП электронного документа. Дополнительно должна быть предусмотрена защита от навязывания, повтора электронного документа и целостность справочников ключей проверки ЭП.

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

- Неотказуемость от передачи электронного документа. Обеспечивается использованием функций ЭП (подпись документа отправителем) и хранением документа с ЭП в течение установленного срока приемной стороной.

- Неотказуемость от приема электронного документа. Обеспечивается использованием функций ЭП и квитированием приема документа (подпись квитанции получателем), хранением документа и квитанции с ЭП в течение установленного срока отправляющей стороной.

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

- Защита от навязывания информации. Защита от нарушителя с целью навязывания им приемной стороне собственной информации, переданной якобы от лица санкционированного пользователя (нарушение авторства информации). Обеспечивается использованием функций ЭП с проверкой атрибутов электронного документа и ключа проверки ЭП отправителя.

- Защита от закладок, вирусов, модификации системного и прикладного ПО обеспечивается совместным использованием криптографических средств, средств антивирусной защиты и организационных мероприятий.

5. Требования к эксплуатации СКЗИ

СКЗИ ЖТЯИ.00091-01 предназначено для защиты открытой информации в информационных системах общего пользования (вычисление/проверка электронной подписи) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах (шифрование/расшифрование информации, вычисление/проверка имитовставки, вычисление значения хэш-функции, вычисление/проверка электронной подписи).

Средствами СКЗИ ЖТЯИ.00091-01 **НЕ ДОПУСКАЕТСЯ** обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

СКЗИ ЖТЯИ.00091-01 **МОЖЕТ ИСПОЛЬЗОВАТЬСЯ** для криптографической защиты персональных данных.

СКЗИ **НЕЛЬЗЯ ИСПОЛЬЗОВАТЬ** для защиты речевой информации без проведения соответствующих дополнительных исследований.

Установочные модули СКЗИ «КриптоПро JCP» версия 2.0 и комплект эксплуатационной документации к нему могут поставляться пользователю Уполномоченной организацией[1] двумя способами:

1. На носителе (CD, DVD - диски);

2. Посредством загрузки через Интернет.

Для получения возможности загрузки установочных модулей СКЗИ «КриптоПро JCP» версия 2.0 и комплекта эксплуатационной документации пользователь направляет свои учетные данные Уполномоченной организации. Учетные данные могут быть направлены посредством заполнения специализированной регистрационной формы на сайте Уполномоченной организации.

После получения Уполномоченной организацией учетных данных пользователю предоставляется доступ на страницу загрузки установочных модулей СКЗИ «КриптоПро JCP» версия 2.0 и комплекта эксплуатационной документации. При загрузке пользователем установочных модулей СКЗИ «КриптоПро JCP» версия 2.0 и комплекта эксплуатационной документации Уполномоченной организацией присваивается учетный номер, идентифицирующий экземпляр СКЗИ «КриптоПро JCP» версия 2.0, предоставленный пользователю.

Вместе с указанными данными на странице загрузки размещаются контрольные суммы установочных модулей и документации. Пользователь, загрузив установочные модули СКЗИ «КриптоПро JCP» версия 2.0 и эксплуатационную, документацию должен убедиться в целостности полученных данных. Это пользователь должен сделать с использованием утилиты cpverify.exe, входящей в состав СКЗИ «КриптоПро JCP» версия 2.0, либо иным другим сертифицированным ФСБ России шифровальным (криптографическим) средством.

Установка СКЗИ «КриптоПро JCP» версия 2.0 на рабочее место пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей СКЗИ «КриптоПро CSP» и эксплуатационной документации.

1. Средство контроля целостности (cpverify.exe) первоначально должно быть получено пользователем на физическом носителе в офисе компании ООО «КРИПТО-ПРО», либо у официального дилера. Такая утилита считается полученной доверенным образом. Далее полученной доверенным образом признается очередная версия утилиты, полученная любым образом, например, скачанная с сайта www.cryptopro.ru, при условии, что она была проверена другим экземпляром утилиты, полученным ранее доверенным образом, и проверка была успешной.

2. Ключ проверки ЭП, а также информация о нем (дата создания, алгоритм хэш-функции, идентификатор алгоритма подписи) записываются в исходный код утилиты на этапе сборки.

[1] Уполномоченная организация – производитель СКЗИ «КриптоПро CSP», либо организация-лицензиат ФСБ России в части распространения шифровальных (криптографических) средств

6. Требования к программной среде

СКЗИ «КриптоПро JCP» версия 2.0 функционирует под управлением следующих Java-машин:

- Java-машина J9VM производства IBM «Java(TM) 2 Runtime Environment, Standard Edition» версии 1.6 и выше на 32-битной и 64-битной платформе.
- Java-машина производства Oracle «Java(TM) 2 Runtime Environment, Standard Edition версии 1.6 и выше на 32-битной и 64-битной платформе.

6.1. СКЗИ предназначено для использования на следующих программно-аппаратных платформах:

Windows

Windows Vista/7/8/8.1/Server 2003/2008 (x86, x64) (только совместно с Java-машиной производства Oracle);

Windows Server 2008 R2/2012/2012 R2 (x64) (только совместно с Java-машиной производства Oracle);

LSB Linux

ОС Linux, удовлетворяющие стандарту Linux Standart Base ISO/IEC 23360 (x86, x64) версии LSB 4.x:

CentOS 4/5/6/7 (x86, x64);

Fedora 23/24/25 (x86, x64);

Mandriva Enterprise Server 5, Business Server 1 (x86, x64);

Oracle Linux 5/6/7 (x86, x64);

OpenSUSE 12.2/12.3/13.1/13.2 (x86, x64);

SUSE Linux Enterprise 10/11/12 (x86, x64, POWER);

Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER);

Ubuntu 10.04/12.04/12.10/13.04/14.04/14.10/15.04/15.10/16.04/16.04.1/16.10 (x86, x64, POWER);

Linux Mint 13/14/15/16/17/18 (x86, x64);

Debian 7/8 (x86, x64, POWER);

Unix

ALT Linux 6/7 (x86, x64);

ALT Linux 6/7 (ARM) (только совместно с Java-машиной производства Oracle);

Ubuntu Phone (ARM) (только совместно с Java-машиной производства Oracle);

ROSA 2011, Enterprise Desktop X.1 (Marathon), Enterprise Linux Server (x86, x64);

РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);

FreeBSD 8/9/10, pfSense 2.x (x86, x64);

AIX 5/6/7 (POWER) (только совместно с Java-машиной производства IBM);

Mac OS X 10.7/10.8/10.9/10.10/10.11/10.12 (x64);

Solaris 10 (sparc, x86, x64) (только совместно с Java-машиной производства Oracle);

Solaris 11 (sparc, x64) (только совместно с Java-машиной производства Oracle).

7. Исполнения СКЗИ

Исполнение 1 класса защиты КС1 выполнено в составе:

криптопровайдер (модуль на прикладном уровне);

модуль обработки сертификатов и CMS протокола;

библиотека, обеспечивающая подключение и функционирование ключевых носителей (RDK);

модуль поддержки интерфейса под управлением виртуальной Java-машины,

набор модулей и Java-классов для поддержки Java JCA интерфейса.

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

Исполнение 2 класса защиты КС1 выполнено в составе:

криптопровайдер (модуль на прикладном уровне);

модуль шифрования;

модуль сетевой аутентификации (КриптоПро JTLS);

модуль обработки сертификатов и CMS протокола;

библиотека, обеспечивающая подключение и функционирование ключевых носителей (RDK);

модуль поддержки интерфейса под управлением виртуальной Java-машины,

набор модулей и Java-классов для поддержки Java JCA интерфейса.

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

8. Реализуемые алгоритмы

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

Алгоритм проверки ЭП реализован в соответствии с ГОСТ Р 34.10 2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной подписи".

Алгоритм проверки ЭП реализован в соответствии с ГОСТ Р 34.10 2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной подписи".

Алгоритм формирования ЭП реализован в соответствии с ГОСТ Р 34.10 2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной подписи".

Алгоритм формирования ЭП реализован в соответствии с ГОСТ Р 34.10 2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной подписи".

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

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

Ключевая система СКЗИ «КриптоПро JCP» версия 2.0 обеспечивает возможность парно-выборочной связи абонентов сети с использованием для каждой пары абонентов уникальных ключей, создаваемых на основе принципа открытого распределения ключей.

9. Архитектура ПО и общие принципы функционирования

Основной архитектурной особенностью ПО СКЗИ «КриптоПро JCP» версия 2.0 является то, что СФК не имеет непосредственного доступа к ключевой и криптографически значимой информации. Все операции с закрытыми ключами, незавершенными значениями хэш-функций и т. п. осуществляется недоступные пользователю объектов; операции экспорта отсутствуют.

9.1. Состав программного обеспечения

В состав программного обеспечения для всех платформ входят СКЗИ «КриптоПро JCP» версия 2.0 и СФК.

Общая структура СКЗИ «КриптоПро JCP» версия 2.0 представлена на Рисунок 1.

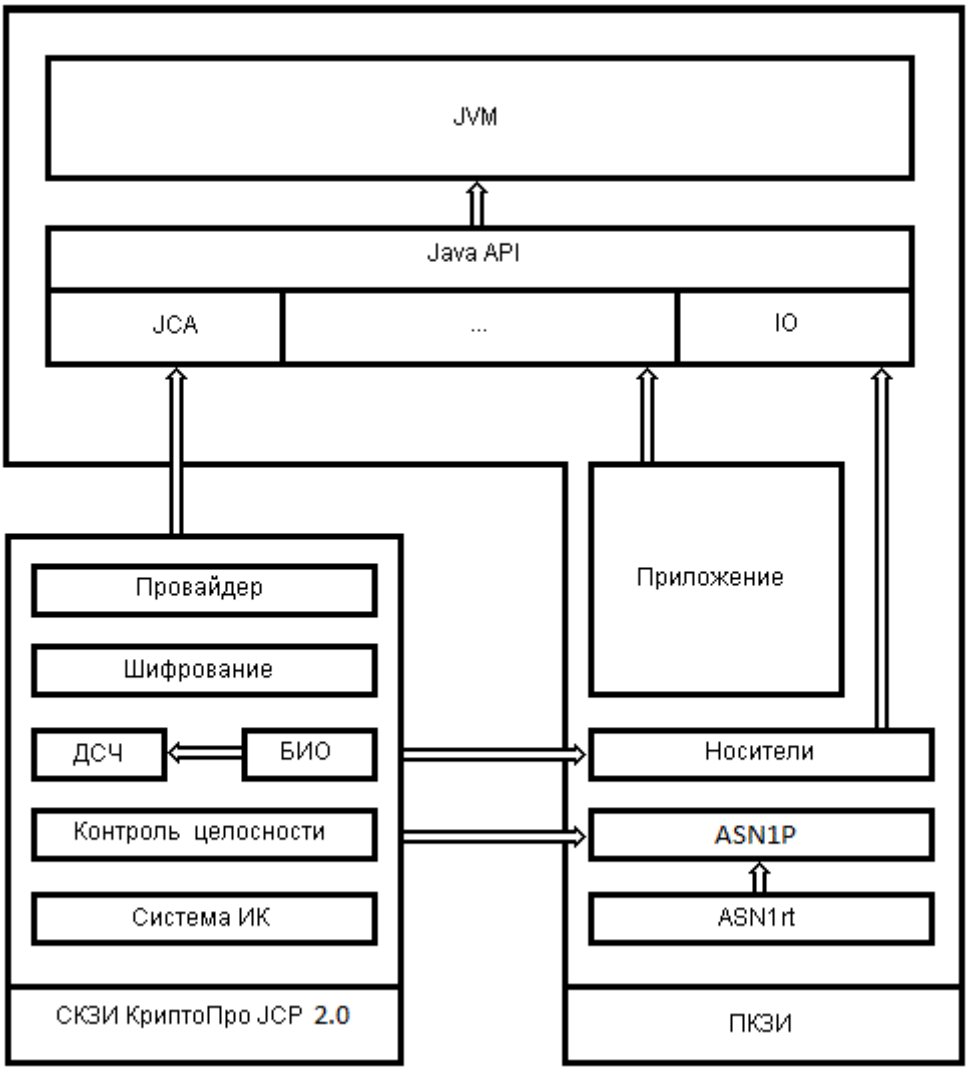

Рисунок 1. Состав программного обеспечения

9.2. СКЗИ «КриптоПро JCP» версия 2.0

В состав СКЗИ «КриптоПро JCP» версия 2.0 входят:

- Библиотеки криптопровайдера для исполнений по уровню КС1;
- Библиотеки шифровального провайдера для исполнений по уровню КС1;
- Подсистема контроля целостности;

- Датчик случайных чисел (ДСЧ);
- Биологический датчик случайных чисел для инициализации основного ДСЧ.

9.3.СФК

В состав СФК входят следующие компоненты:

- ASN.1 модуль;
- Модуль поддержки ASN.1;
- Модуль запроса сертификатов;
- Подсистема настройки провайдера;
- Модули поддержки считывателей и носителей;
- Java-машина.

10. Ключевая система

10.1. Общие положения

СКЗИ «КриптоПро JCP» версия 2.0 является системой с открытым распределением ключей. Ключи проверки подписи обычно представляются в виде сертификатов ключей проверки подписи.

В СКЗИ «КриптоПро JCP» версия 2.0 ключ электронной подписи может быть использован только для формирования ЭП. Закрытый ключ шифрования может быть использован как для формирования ключа связи с другим пользователем, так и для формирования ЭП.

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

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

10.2. Шифрование данных

В СКЗИ «КриптоПро JCP» версия 2.0 ключ зашифрования сообщения совпадает с ключом расшифрования (общий закрытый ключ связи). При зашифровании сообщения пользователя А для пользователя Б общий закрытый ключ связи вырабатывается на основе закрытого ключа шифрования пользователя А и открытого ключа шифрования пользователя Б. Соответственно, для расшифрования этого сообщения пользователем Б формируется общий закрытый ключ связи на основе своего собственного закрытого ключа шифрования и открытого ключа шифрования пользователя А.

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

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

10.3. Формирование и проверка ЭП

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

- ключ электронной подписи;
- ключи проверки подписи (сертификаты ключей проверки электронной подписи) других пользователей.

10.4. Ключевой контейнер

При формировании закрытые ключи СКЗИ «КриптоПро JCP» версия 2.0 записываются на ключевой носитель (ключевой контейнер).

Ключевой контейнер может содержать:

- только ключ электронной подписи;

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

«КриптоПро JCP» версия 2.0 может создавать ключевой контейнер, состоящий только из ключа подписи или только из ключа шифрования. При создании ключа, если существует контейнер с тем же именем (alias), то он будет уничтожен и на его место будет создан новый контейнер.

Если ключевой контейнер был создан, не с помощью «КриптоПро JCP» версия 2.0 (например, при помощи КриптоПро CSP), то в качестве ключа для выработки ЭП будет использоваться

- ключ электронной подписи, если контейнер содержит ключ подписи
- ключ шифрования, если контейнер не содержит ключа подписи

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

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

10.5. Структура ключевого контейнера

Ключевой контейнер содержит следующую информацию: главный ключ, маски главного ключа, контрольную информацию главного ключа, вторичный ключ (опциональный), резервную копию ключевого контейнера.

Каждый закрытый ключ или ключ ЭП хранится в формате, дополнительно содержащем все константы, необходимые для формирования открытого ключа или ключа проверки ЭП.

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

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

10.6. Формирование ключей

1. Ключи ЭП и шифрования формируются с использованием программного ДСЧ с инициализацией от биологического ДСЧ (клавиатура-мышь), обеспечивающих защиту по уровню КС1;
2. При использовании считывателей смарт-карт необходимо произвести настройки OpenCard Framework;
3. Перед использованием процессорные карты должны быть "выпущены" с использованием транспортного пин-кода и ПО выпуска карт (поставляются дистрибутором карт);
4. При использовании НГМД в качестве ключевого носителя во избежание потери ключевой информации рекомендуется хранить ее копию.

10.7. Хранение ключевых носителей

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

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

Требования по хранению личных ключевых носителей распространяются на ПЭВМ (в том числе и после удаления ключей с диска).

Настоятельно рекомендуется использовать парольную защиту при хранении ключей на ЖМД.

При необходимости передачи ключевого носителя постороннему, информацию с него необходимо гарантированно удалить.

10.8. Сроки действия ключей

При использовании ключей обязательным является выполнение условий:

- максимальный срок действия закрытых ключей шифрования и ключей ЭП - 1 год 3 месяца;
- максимальный срок действия открытых ключей шифрования - 1 год 3 месяца;
- срок действия сертификата ключа проверки ЭП пользователя - не больше 5 лет;
- максимальный срок действия ключей проверки ЭП при использовании алгоритма ГОСТ Р 34.10-2001 - 15 лет;
- максимальный срок действия ключей проверки ЭП при использовании алгоритма ГОСТ Р 34.10-2012 (256) - 15 лет.

10.9. Уничтожение ключей на ключевых носителях

Ключи на ключевых носителях (включая смарт-карты), срок действия которых истек, уничтожаются путем удаления ключевых контейнеров средствами ПО СКЗИ или с помощью Контрольной Панели, после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

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

10.10. Интерфейс управления ключами СКЗИ

Управление ключами может осуществляться при помощи программы keytool входящей в состав Java 2 Runtime или при помощи прикладного программного обеспечения (см. «Использование утилиты keytool»).

11.Усиленный контроль использования ключей.

Режим усиленного контроля использования ключей обеспечивает осуществление контроля срока действия долговременных ключей электронной подписи и ключевого обмена, контроля доверенности ключей проверки электронной подписи и контроля корректного использования программного датчика случайных чисел. Данный режим должен быть **в обязательном порядке включён** при инсталляции СКЗИ, либо через контрольную панель «КриптоПро JCP» версия 2.0 (вкладка «Дополнительно») после инсталляции СКЗИ.

Внимание! Работа СКЗИ при отключённом режиме усиленного контроля использования ключей допускается исключительно в тестовых целях.

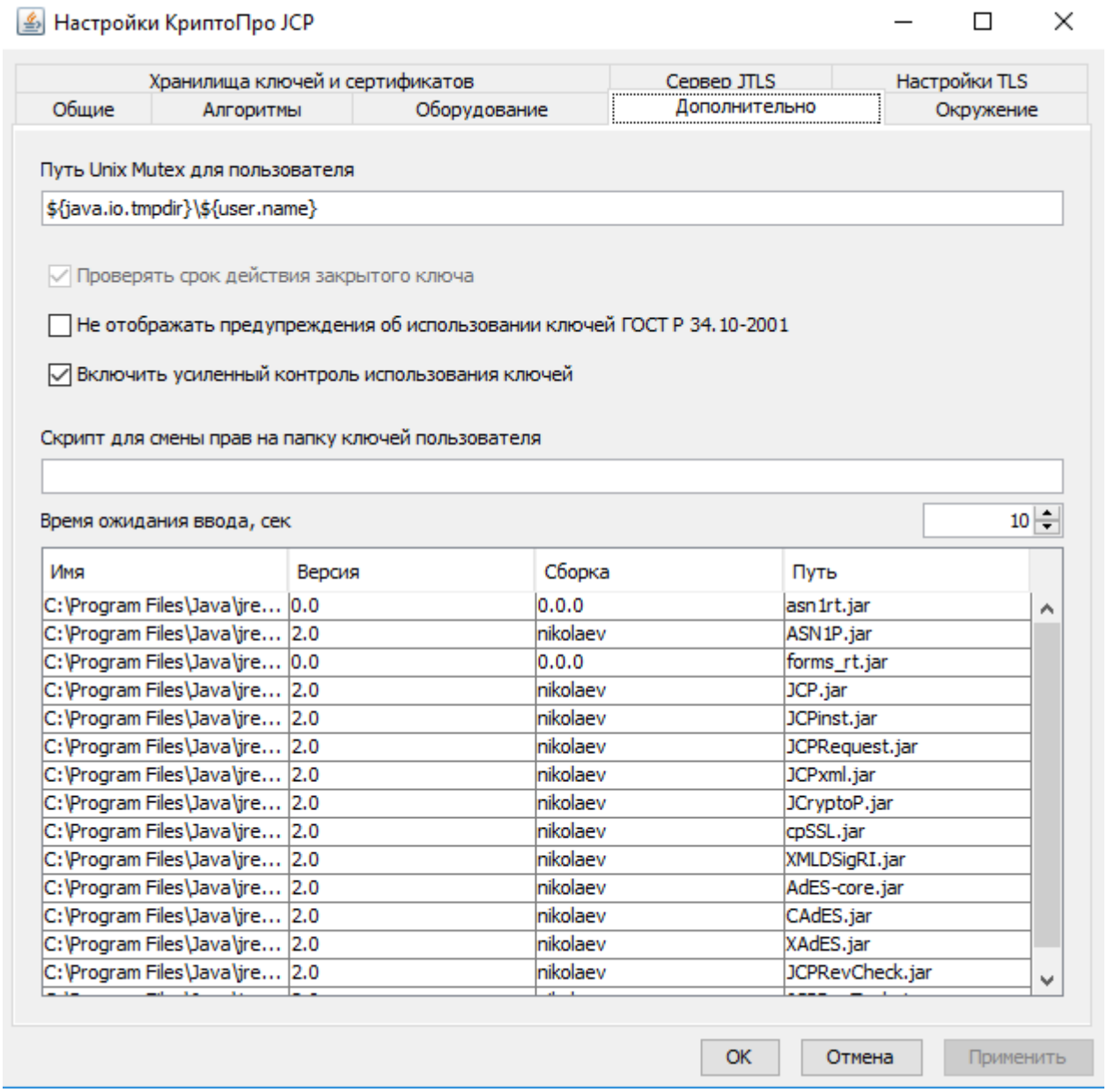

Рисунок 2. Включение режима усиленного контроля использования ключей.

12.Ключевые носители

Формирование закрытых ключей и ключей ЭП может производиться на следующие ключевые носители:

- дискета 3,5";
- российские интеллектуальные карты (Оскар) с использованием считывателей смарт-карт, поддерживающих интерфейс OpenCard Framework (в том числе протокол PS/SC для Windows);
- сменный носитель с интерфейсом USB (eToken, JaCarta, Rutoken);
- Директорию жёсткого диска.

Примечания.

1. Перечень ключевых носителей уточняется (см. Формуляр ЖТЯИ.00091-01 30 01).

2. Перечень ключевых носителей может расширяться.

1.2. Размеры ключей

Размеры ключей электронной подписи:

- ключ электронной подписи - 256 бит;
- ключ проверки электронной подписи -
  - 512 бит на базе алгоритма ГОСТ Р 34.10 2001
  - 512 бит на базе алгоритма ГОСТ Р 34.10 2012 (256)
  - 1024 бит на базе алгоритма ГОСТ Р 34.10 2012 (512)

Размеры ключей, используемых при шифровании:

- закрытый ключ - 256 бит;
- открытый ключ -
  - 512 бит на базе алгоритма ГОСТ Р 34.10 2001
  - 512 бит на базе алгоритма ГОСТ Р 34.10 2012 (256)
  - 1024 бит на базе алгоритма ГОСТ Р 34.10 2012 (512)
- симметричный ключ - 256 бит;

Возможна ситуация, когда установленная JRE имеет экспортные ограничения. США запрещает экспорт "сильной" криптографии и «КриптоПро JCP» версия 2.0 с длиной ключа 256 или 512 бит попадает под это ограничение. Ограничения устанавливаются файлами local_policy.jar и US_export_policy.jar в каталоге <JRE>/jre/lib/security. Для снятия экспортных ограничений необходимо скачать файл jce_policy.zip с политиками со страницы http://www.oracle.com/technetwork/java/javase/downloads/index.html, выбирая "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files" версии 6 или 7. Для отладки же можно просто скопировать US_export_policy.jar в local_policy.jar (оба файла должны присутствовать).

1.3. Совместимость с продуктами КриптоПро

«КриптоПро JCP» версия 2.0 позволяет:

- чтение криптопровайдером «КриптоПро JCP» версия 2.0 ключей, созданных при помощи криптопровайдера КриптоПро CSP 3.0 и выше, с ключевых носителей, и наоборот;
- копирование с ключевых носителей криптопровайдером «КриптоПро JCP» версия 2.0 ключей, созданных при помощи криптопровайдера КриптоПро CSP 3.0 и выше, на другие ключевые носители, и наоборот;

- чтение сертификатов удостоверяющего центра КриптоПро УЦ;
- чтение сертификатов удостоверяющего центра Microsoft CA с установленным на нем СКЗИ КриптоПро CSP 2.0 и выше;
- создание при помощи класса GostCertificateRequest запроса для удостоверяющего центра Microsoft CA с установленным на нем СКЗИ КриптоПро CSP 2.0 и выше, а также для удостоверяющего центра КриптоПро УЦ 1.3 и выше;
- создание при помощи утилиты keytool запроса для удостоверяющего центра Microsoft CA с установленным на нем СКЗИ КриптоПро CSP 2.0 и выше, а также для удостоверяющего центра КриптоПро УЦ 1.4.

СКЗИ «КриптоПро JCP» версия 2.0 совместимо с КриптоПро CSP 3.6, 3.6.1, 3.8, 3.9 и 4.0 по выполняемым криптографическим функциям, форматам данных и ключам со следующими ограничениями:

- не поддерживается атрибут CRYPT_USER_PROTECTED;
- не поддерживаются двухключевые контейнеры и контейнеры с разделённым хранением закрытого ключа на разных ключевых носителях;
- не поддерживается управление контейнером "по умолчанию" на ключевом носителе;
- недопустима одновременная работа КриптоПро CSP и «КриптоПро JCP» версия 2.0 с одним и тем же контейнером в ОС Windows.

СКЗИ «КриптоПро JCP» версия 2.0 совместимо с КриптоПро CSP 3.0 по выполняемым криптографическим функциям, форматам данных и ключам со следующими, дополнительными к 3.6 ограничениями:

- не поддерживаются операции с закрытыми ключами ГОСТ Р 34.10-94.

СКЗИ «КриптоПро JCP» версия 2.0 совместимо с КриптоПро CSP 2.0 только по выполняемым криптографическим функциям и форматам данных со следующими, дополнительными к 3.0 ограничениями:

- не поддерживаются ключевые контейнеры, созданные КриптоПро CSP 2.0.

СКЗИ «КриптоПро JCP» версия 2.0 совместимо с КриптоПро УЦ 1.3/1.4/1.5/2.0 по форматам данных со следующими ограничениями:

- требуется использовать дополнительный CertPathValidator (см. «Руководство программиста») в случае использования COC (CRL) и без регламентного изменения различительного имени при плановой смене ключа УЦ (X.500 DN) (расширение Microsoft szOID_CERTSRV_CA_VERSION "1.3.6.1.4.1.311.21.1" не поддерживается стандартными CertPathValidator и CertPathBuilder)

В СКЗИ КриптоПро CSP версии 3.0 на Unix-системах ключи хранились в каталоге /var/cCPROcsp/keys/${user.name}. В СКЗИ КриптоПро CSP версии 3.6 ключи хранятся /var/opt/cprocsp/keys/${user.name}. Пути к блокировкам соответственно поменялись с /var/CPROcsp/tmp на /var/opt/cprocsp/tmp.

Если Вы используете на одном компьютере и «КриптоПро JCP» версия 2.0, и CSP необходимо настроить пути к ключам в соответствии в версией СКЗИ КриптоПро CSP. Это можно сделать средствами контрольной панели, из командной строки или программно.

СКЗИ «КриптоПро JCP» версия 2.0 совместимо с КриптоПро PDF при условии использования PDF с расширенными правами. Такой PDF можно сделать, например, в Adobe LiveCycle и Adobe Acrobat Pro. Для создания подписи в файле формата PDF с расширенными правами с помощью СКЗИ «КриптоПро JCP» версия 2.0 можно, например, использовать свободную библиотеку iText. Такая подпись будет видна в PDF-файле при просмотре через Adobe Reader, а если установлены СКЗИ «КриптоПро JCP» версия 2.0 и КриптоПро PDF, то она сможет проверяться.

13.Управление ключами СКЗИ

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

Рекомендации по управлению ключами приведены для КриптоПро УЦ, основанные на использовании сертификатов ключей проверки и, исходя из наличия, определенные организационной структурой управления ключами, элементами которой являются:

- Центр сертификации центр (ЦС)
- Центр регистрации (ЦР)
- АРМ администратора
- Пользовательские средства взаимодействия с УЦ
- Программный интерфейс взаимодействия с УЦ

Примечание.

СКЗИ «КриптоПро JCP» версия 2.0 может использоваться в качестве криптоядра в составе различных прикладных систем, организационные схемы управления ключевой системой которых могут отличаться от рассматриваемой.

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

1. имя субъекта или объекта системы, однозначно идентифицирующее его в системе;
2. ключ проверки ЭП субъекта или объекта системы;
3. дополнительные атрибуты, определяемые требованиями использования сертификата в системе;
4. ЭП Издателя (Удостоверяющего центра), заверяющую совокупность этих данных.

Формат сертификата определен в соответствии с Технической спецификацией использования алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509.

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

13.1.Удостоверяющий центр

Удостоверяющий центр является структурным подразделением, обеспечивающим выполнение следующих функций:

- регистрация (формирование) дистрибутивов ПО СКЗИ и выдача их пользователям;
- формирование, хранение и использование ключа (ключей) ЭП Центра Сертификации;
- регистрация пользователей в соответствии с требованиями Регламента (Договора) системы;
- получение от пользователя запроса на сертификат, как в электронном, так и в бумажном виде;
- верификация запроса на сертификат;
- формирование сертификатов ключей проверки ЭП пользователей на основе полученных запросов и зарегистрированной информации;

- доставка сертификатов ключей проверки ЭП пользователям;
- получение и обработка сообщений о компрометации ключей пользователями;
- организация схемы оперативного оповещения пользователей обо всех изменениях, происходящих в сети (компрометация ключей, восстановление конфиденциальной связи после компрометации ключей, включение новых пользователей, плановая смена ключей и т. п.);
- плановое изготовление списка отозванных сертификатов;
- разработка и поддержка функционирования парольной системы оповещения в сети;
- управление ключевой системой;
- разбор конфликтных ситуаций и доказательство авторства электронного документа, снабженного электронной подписью.
- В состав программно-аппаратных средств УЦ входят:
- программно-аппаратные средства Центра Сертификации;
- программно-аппаратные средства Центра Регистрации (при условии его эксплуатации на отдельной ПЭВМ);
- программно-аппаратные средства для разбора конфликтных ситуаций;
- дополнительные средства, обеспечивающие сетевое взаимодействие пользователей и УЦ.

13.2.Формирование ключей Центра Сертификации

Формирование ключей Центра Сертификации производится администратором ЦС следующим образом:

1. Администратор ЦС регистрируется в УЦ в "Журнале регистрации администраторов безопасности и пользователей" (см. «Ведение журналов»). Регистрацию проводит начальник УЦ (о чем делается соответствующая отметка в журнале).
2. Администратор ЦС производит формирование ключа ЭП ЦС и сертификата о ключа проверки ЭП ЦС. С ключа ЭП ЦС формируется резервная копия, которая хранится у начальника УЦ. Факт изготовления ключа и сертификата ЦС заносится в "Журнале пользователя сети" и заверяется начальником УЦ.
3. Бланк сертификата ЦС выводится на принтер в двух экземплярах и заверяется начальником УЦ и администратором ЦС. Одна копия бланка сертификата ЦС хранится и начальника УЦ, вторая копия передается администратору ЦР (ЦС).
4. Администратор ЦС производит формирование СОС ЦС, который не содержит ни одного отозванного сертификата. Бланк СОС выводится на принтер в двух экземплярах и заверяется администратором ЦС. Одна копия бланка СОС ЦС хранится и начальника УЦ, вторая копия передается администратору ЦР (ЦС).

Примечание.

При формировании СОС ЦС и наличии сетевых средств распространения СОС в системе, рекомендуется установить в СОС дополнение Точка распространения СОС (issuingDistributionPoint) с заданием в нем метода доступа, который может быть использован пользователями для регулярного обновления СОС (см. [PKIX], [X.509]).

13.2.1.Ключ ЭП и сертификат ЦС

При формировании ключа ЭП и сертификата ЦС рекомендуется использовать следующие значения. Сроки действия:

- срок действия ключа ЭП ЦС, предназначенный для формирования ЭП сертификатов ключей проверки ЭП - до 5 лет;
- срок действия сертификата ЦС - не больше 10 лет.

13.3. Хранение и использование ключа ЭП ЦС

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

13.4. Формирование ключей Центра Регистрации

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

13.4.1. Регистрация Центра Регистрации

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

13.4.2. Ключ и сертификат ЦР

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

Сроки действия:

- срок действия ключа ЭП ЦР - 1 год 3 месяца;
- срок действия сертификата ЦР - не больше 5 лет.

13.4.3. Изготовление ключей Центра Регистрации

1. Администратор ЦР устанавливает сертификат ЦС на ПЭВМ ЦР. Рекомендуется обеспечить защищенную доставку и хранение сертификата ЦС на ПЭВМ.

2. Администратор ЦР производит формирование личного ключа ЭП ЦР и запроса на сертификат, содержащего ключ проверки ЭП ЦР. С ключа ЭП ЦР формируется резервная копия, которая хранится у начальника УЦ. Пометка о формировании ключа и запроса на сертификат заносится в "Журнале пользователя сети".

3. Бланк запроса на сертификат выводится на принтер в двух экземплярах и заверяется администратором ЦР.

4. Запрос на сертификат записывается на магнитный носитель (дискету).

5. Администратор ЦР прибывает в УЦ, где администратор ЦС производит формирование сертификата ЦС, используя для этого полученный запрос на сертификат и бумажный бланк запроса. Бланк запроса на сертификат заверяется администратором ЦС. Одна копия бланка запроса хранится у администратора ЦС, другая - у администратора ЦР.

6. Администратор ЦС выводит на принтер бланк сертификата ЦР в двух экземплярах. Бланк сертификата ЦР сверяется с бланком запроса и заверяется администраторами ЦС, ЦР и начальником УЦ.

7. Администратор ЦР получает личный сертификат ЦР на магнитном носителе и заверенный бланк сертификата ЦР.

8. Администратор ЦР, используя ПО ЦР, устанавливает сертификат на ПЭВМ ЦР.

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

13.5. Формирование ключей пользователя

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

1. регистрация пользователя;
2. формирование пользователем личных ключей (запроса на сертификат);
3. передача запроса в Центр Регистрации;

4. верификация запроса Центром Регистрации;
5. формирование сертификата пользователя;
6. получение сертификата пользователям.

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

1. лист с образцами печати и личной подписи руководителя организации;
2. копию Договора (Временного соглашения) с администрацией системы;
3. выписку из приказа о назначении администратора информационной безопасности организации (заместителя), заверенную подписью руководства и печатью организации;
4. заполненные и заверенные листки по учету кадров на администратора безопасности организации (заместителя).

Формирование ключей пользователя происходит в следующей последовательности.

13.5.1.Регистрация пользователя

1. Пользователя системы или администратор безопасности, прибывают в Удостоверяющий Центр (Центр Регистрации) с документами, необходимыми для регистрации пользователя в системе.
2. Администратор Центра Регистрации на основании полноты и достаточности предоставленных документов производит регистрацию пользователя в системе.
3. Данные регистрации пользователя выводится на принтер в двух экземплярах и заверяется администратором ЦР и пользователем. Один экземпляр бланка регистрации хранится у администратора ЦР, второй экземпляр - у пользователя.
4. Администратор ЦР выдает пользователю карточку оповещения о компрометации, в которой отражаются телефоны и пароли УЦ и пользователя. В Карточке оповещения указаны: телефоны УЦ, пароль (кодовое слово) администратора УЦ, уникальный пароль (кодовое слово), присвоенный пользователю УЦ.
5. При наличии системы электронной почты и зарегистрированного почтового адреса пользователя, администратор ЦР добавляет его в список рассылки пользователей системы, который используется для централизованного оповещения пользователей системы.
6. Администратор ЦР делает запись в "Журнале регистрации администраторов безопасности и пользователей".

Примечание.

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

Карточка оповещения о компрометации

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

Примечание.

Карточка оповещения используется участниками системы для сообщений о компрометации ключа по телефонным каналам общего пользования. Карточка оповещения должна храниться у пользователя наравне с ключами.

13.5.2.Ключ и сертификат пользователя

При формировании ключа электронной подписи и сертификата ключа проверки ЭП пользователя следует использовать следующие значения.

Сроки действия:

- срок действия ключа ЭП пользователя- до 1 года 3 месяцев;
- срок действия сертификата ключа проверки ЭП пользователя - не больше 5 лет.

13.5.3.Формирование личных ключей пользователя

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

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

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

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

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

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

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

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

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

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

13.5.4.Получение личного сертификата пользователем

Личный сертификат может быть получен следующими способами:

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

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

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

13.6.Повторная регистрация пользователя

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

13.7.Плановая смена ключей

13.7.1.Смена ключей Центра Сертификации

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

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

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

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

13.7.2.Смена ключей Центра Регистрации

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

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

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

13.7.3.Смена ключей пользователя

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

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

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

13.8.Компрометация ключей

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

По факту компрометации ключей должно быть проведено служебное расследование.

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

13.8.1.Компрометация ключей Центра Сертификации

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

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

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

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

13.8.2.Компрометация ключей Центра Регистрации

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

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

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

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

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

13.8.3.Компрометация ключей пользователя

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

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

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

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

13.8.4.Действия УЦ при компрометации ключей пользователя

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

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

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

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

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

13.9.Исключение пользователя из сети

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

13.10.Периодичность издания СОС

Периодичность издания СОС Центром Сертификации определяется администрацией системы.

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

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

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

13.11. Ведение журналов

Администратор УЦ ведет следующие журналы:

- "Журнал регистрации администраторов безопасности и пользователей",
- "Журнал пользователя сети",

Администраторы безопасности организации ведут журнал "Журнал пользователя сети".

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

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

В "Журнале пользователя сети" может отражаться следующая информация:

- дата, время;
- запись о компрометации ключа;
- запись об изготовлении личного ключевого носителя пользователя, идентификатор носителя;
- запись об изготовлении копий личного ключевого носителя пользователя, идентификатор носителя;
- запись об изготовлении резервного ключевого носителя пользователя, идентификатор носителя;
- запись о получении сертификата ключа проверки ЭП, полный номер ключевого носителя, соответствующий сертификату;
- записи, отражающие выдачу на руки пользователям (ответственным исполнителям) и сдачу ими на хранение личных ключевых носителей, включая резервные ключевые носители;
- события, происходившие на АРМ пользователя с установленным ПО СКЗИ, с указанием причин и предпринятых действий;

Примечание.

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

14. Требования по встраиванию и использованию ПО СКЗИ

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

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

Следует отметить, что вновь разрабатываемые СФК и прикладное ПО, использующие сертифицированные СКЗИ должны удовлетворять требованиям к СКЗИ в части корректности использования СКЗИ и проверки влияния на СКЗИ со стороны ПО. Поэтому, в соответствии с российскими законами, встраивание СКЗИ могут производить организации, имеющие лицензию на право проведения таких работ, а работы по встраиванию должны проводиться в соответствии с Положением ПКЗ 2005 [ПКЗ-2005].

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

СКЗИ «КриптоПро JCP» версия 2.0 в первую очередь предназначено для встраивания в прикладное программное обеспечение. Функции СКЗИ «КриптоПро JCP» версия 2.0, могут быть использованы:

- через интерфейс функций JCA, что позволяет применять весь инструментарий Java. Для этих целей разработчики могут воспользоваться программной документацией, содержащейся в Java 2 SDK, а также поставляемым тестовым ПО. Для этих целей в комплект поставки включается документ ЖТЯИ.00091-01 33 01 "КриптоПро JCP. Руководство программиста".
- в стандартном прикладном ПО Java.

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

Конфиденциальность информации

Конфиденциальность информации при передаче данных в сети обеспечивается использованием функций шифрования. Для обеспечения защиты от НСД к информации при хранении (на дисках, в базе данных) допускается использование шифрования на производном (например, от пароля) ключе.

Идентификация и авторство

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

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

Целостность

Целостность обеспечивается использованием функций ЭП электронного документа. При использовании функций шифрования (без использования ЭП) обеспечивается имитозащитой.

Для обеспечения целостности хранимых данных может быть использована функция хэширования или имитозащиты, но при этом не обеспечивается авторство информации.

Неотказуемость от передачи электронного документа

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

Неотказуемость от приема электронного документа

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

Защита от переповторов

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

Защита от навязывания информации

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

Защита от закладок, вирусов, модификации системного и прикладного ПО

Обеспечивается совместным использованием криптографических средств и организационных мероприятий (см. «Требования по защите от НСД»).

Правила встраивания и использования СКЗИ «КриптоПро JCP» версия 2.0

При встраивании СКЗИ «КриптоПро JCP» версия 2.0 в прикладное программное обеспечение или использовании его в составе стандартного прикладного ПО должны выполняться следующие требования:

1. При использовании ключей проверки ЭП должна быть обеспечена целостность и идентичность ключа проверки ЭП. Это может быть реализовано:
   - путем заверения ключа проверки ЭП доверенной стороной (например, в случае использования сертификатов ключей проверки подписи);
   - путем доверенного распространения и хранения ключей проверки ЭП в виде справочников.
2. При использовании сертификатов ключей проверки подписи, заверенных подписью доверенной стороны, должна быть обеспечена безопасная доставка и хранение сертификата ключа ЭП доверенной стороны, с использованием которого проверяются остальные сертификаты ключей проверки пользователей.
3. Криптографическое средство, с помощью которого производится заверение ключей проверки ЭП или справочников ключей проверки ЭП, должно быть сертифицировано по классу, соответствующему принятой политике безопасности.
4. Для отзыва (вывода из действия) ключей проверки подписи должны использоваться средства, позволяющие произвести авторизацию отзывающего

лица (в этих целях может быть использован список отозванных сертификатов, заверенный ЭП доверенной стороны).

5. При вызове функций СКЗИ «КриптоПро JCP» версия 2.0 в прикладном программном обеспечении необходимо, при возникновении критических исключений блокировать криптографические вызовы, а при возникновении других исключений, корректно их обрабатывать. (см. руководство программиста)

Совместное использование SunIdM и «КриптоПро JCP» версия 2.0

Sun Java System Identity Manager обеспечивает применение различных алгоритмов ЭП для управлениями правами доступа к информационным ресурсам.

Специалистами компаний Sun Microsystems и КРИТПО-ПРО были совместно выполнены интеграция и тестирование совместной работы Sun Java System Identity Manager со средством криптографической защиты «КриптоПро JCP» версия 2.0.

Произведенная интеграция позволяет использовать реализованные в «КриптоПро JCP» версия 2.0 российские криптографические алгоритмы ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 для заверения российской электронной подписью заявок на получение доступа к ресурсам, используя стандартные интерфейсы в рамках автоматизированного бизнес-процесса системы Sun Java System Identity Manager. Применение российского средства ЭП и сертификатов ключей проверки ЭП гарантирует, что заявка исходит именно от того лица, которое уполномочено на такие действия (руководители, сотрудники службы безопасности и т.д.). Формирование заявок и ЭП производится непосредственно с помощью разработанных web-форм для согласующих лиц. Информация об одобрении заявки, вместе с ЭП, хранится в репозитории Identity Manager и может быть предоставлена в виде отчета, необходимого для проведения аудитов по информационной безопасности.

Для интеграции Sun IdM и «КриптоПро JCP» версия 2.0:

1. Сначала надо установить IdM.

При установке и настройке IdM по документации http://docs.sun.com/source/819-6124/Ch8_java8.html. пункт 3.11 ("Log in to Identity Manager on the port you specified when you installed your applications server.") в процессе установки преждевременный. Сразу входить не надо, сначала надо настроить права по пункту 5.

2. Потом на сервер следует поставить «КриптоПро JCP» версия 2.0 в соответствии с «Рекомендациями по установке ПО СКЗИ».
3. Настроить конфигурацию сервера по документации Configuring Digitally Signed Approvals
    - Для установки `security.nonrepudiation.signedApprovals=true`

Войдите на отладочную страницу Identity Manager http://PathToIDM/debug. Загрузится страница с системными настройками. У пункта "List Objects" надо выбрать из выпадающего меню "Configuration" и нажать "List Objects", появится страница "List Objects of type: Configuration". У пункта "System Configuration" надо выбрать "Edit", появится файл содержащий системную конфигурацию. Его надо отредактировать, установив signedApprovals=true.

```
<Attribute name='nonrepudiation'>
    <Object>
        <Attribute name='signedApprovals'>
        <Boolean>true</Boolean>
     </Attribute>
    </Object>
</Attribute>
```

- Установка сертификатов из интерфейса администратора.

  В документации сказано: "From the Administrator interface, select Configure, and then select Certificates". В седьмой версии пункт меню Sertificates реально находится в меню Security.

- Подпись applets/ts1.jar с использованием jarsigner.

  Именно ts1.jar проставляет подпись на клиенте. Подпись не на ГОСТ-овских алгоритмах, нужна для того, чтобы разрешить выполнение кода на клиентской машине.

4. Добавить алгоритмы «КриптоПро JCP» версия 2.0 в IdM.

В файле `samples_src.jar` в каталоге SunIdM находятся две модифицированные формы IdM: "Approval Form.xml" и "Work Item Configuration.xml". В них добавлены параметры `supportedKeyStoreTypes` и `keytypeSignatureMapping` для полей типа TransactionSigner.

```
<Property name='keytypeSignatureMapping'
value='DSA=SHA1withDSA,RSA=SHA1withRSA,RSA=MD5withRSA,RSA=MD2withRSA,GOST3
410=GOST3411withGOST3410EL'/>

<Property name='supportedKeyStoreTypes' value='JKS,PKCS12,HDImageStore'/>
```

Надо установить в поле `supportedKeyStoreTypes` типы хранилищ ключей, которые будут использованы на клиентской машине для подписи. `HDImageStore` добавлен для примера, установите типы хранилищ, которые будут реально использоваться. Эти формы необходимо по очереди импортировать в конфигурацию через web-интерфейс, Configure -> Import Exchange File. Перезагрузите IdM.

5. Установить «КриптоПро JCP» версия 2.0 на клиенте.

Подготовьте хранилища и ключи, которые будут использоваться для подписи. Указания "Obtain a certificate and private key, and then export them to a PKCS#12 keystore." необходимо игнорировать. «КриптоПро JCP» версия 2.0 и PKCS#12 несовместимы.

15.Порядок разбора 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 алгоритма ЭП, реализованного в соответствии со стандартами Российской Федерации ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, гарантирующими невозможность подделки значения ЭП любым лицом, не обладающим ключом электронной подписи.

При проверке значения ЭП используется ключ проверки, 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 системы (Договору), заключаемому между участниками автоматизированной системы.

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

15.1.Порядок разбора конфликтной ситуации

Разбор конфликтной ситуации выполняется по инициативе любого участника автоматизированной системы и состоит из:

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

Разбор конфликтной ситуации проводится с использованием программного обеспечения СКЗИ «КриптоПро JCP» версия 2.0 для электронного документа, авторство или содержание которого оспаривается.

Проверка подписанного электронного документа включает в себя выполнение следующих действий:

1. определение сертификата или нескольких сертификатов, необходимых для проверки ЭП;

2. проверка ЭП электронного документа с использованием каждого сертификата;

3. определение даты формирования каждой ЭП в электронном документе;

4. проверка ЭП каждого сертификата, путем построения цепочки сертификатов до сертификата Главного ЦС;

5. проверка действительности сертификатов на текущий момент времени;

6. проверка действительности сертификатов на момент формирования ЭП;

7. проверка отсутствия сертификатов в СОС.

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

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

15.2. Случаи невозможности проверки значения ЭП

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

16.Нештатные ситуации при эксплуатации СКЗИ

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

Нештатная ситуация	**Действия персонала**
Эвакуация, угроза нападения, взрыва и т.п., стихийные бедствия, аварии общего характера в Центре управления ключевой системой.	Остановить все ЭВМ. Персонал, имеющий доступ к ключам, обязан сдать все имеющиеся у него в наличии ключевые носители администратору безопасности. Администратор безопасности упаковывает все ключевые носители, регистрационные карточки сертификатов 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.
Компрометация одного из личных ключевых носителей.	Порядок действий при компрометации ключей описан в разделе «Компрометация ключей пользователя».
Выход из строя первого личного ключевого носителя. Аналогично для смарт-карт.	Необходимо сообщить по телефону в УЦ о факте выхода из строя личного ключевого носителя и обеспечить его доставку в УЦ для выяснения причин выхода из строя. Для работы используется второй личный ключевой носитель.
Выход из строя второго личного ключевого носителя (при условии, что первый тоже вышел из строя).	Пользователь, у которого вышли из строя оба личных ключевых носителя, является в УЦ для повторной регистрации (без изменения данных регистрации).
Отказы и сбои в работе аппаратной части АРМ со встроенной СКЗИ.	При отказах и сбоях в работе аппаратной части АРМ со встроенной СКЗИ необходимо остановить работу, по возможности локализовать неисправность и в дальнейшем произвести ремонт в установленном порядке и, при необходимости, переустановку СКЗИ.
Отказы и сбои в работе средств защиты от НСД.	При отказах и сбоях в работе средств защиты от НСД, администратор безопасности, должен восстановить работоспособность средств НСД. При необходимости переустановить программно-аппаратные средства НСД.
Утеря личного ключевого носителя.	Утеря личного ключевого носителя приводит к компрометации ключей. Порядок действий при компрометации ключей описан в разделе «Компрометация ключей пользователя».
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. Перед продолжением работы следует в обязательном порядке произвести перезапуск компьютера.
Отказы в работе программных средств вследствие случайного	При отказах в работе программных средств, вследствие случайного или умышленного их повреждения, лицо, ответственное за

или умышленного их повреждения.	безопасность функционирования программных и аппаратных средств, обязано произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы программных средств в установленном порядке.
Отказы в работе программных средств вследствие ошибок оператора.	При отказах в работе программных средств, вследствие ошибок оператора, оператор сообщает о данном факте лицу, ответственному за безопасность функционирования программных и аппаратных средств. Ответственный за безопасность функционирования программных и аппаратных средств дает соответствующие указания обслуживающему персоналу по восстановлению правильной работы программных средств в установленном порядке.

Все нештатные ситуации должны отражаться в "Журнале пользователя сети" (см. «Ведение журналов»).

17.Установка ПО СКЗИ на ПЭВМ

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

Установка СКЗИ на рабочее место пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей СКЗИ и эксплуатационной документации (п.п. 20,21).

При установке программного обеспечения СКЗИ, необходимо:

1. На технических средствах, оснащенных СКЗИ, использовать только лицензионное программное обеспечение фирм-изготовителей.
2. Установленное программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.
3. Аппаратуру, на которой устанавливается СКЗИ, следует получать у добросовестного производителя, проверяя наличие подтверждающих работоспособность документов.
4. Рекомендуется установка средств защиты от НСД и при использовании СКЗИ в соответствии с классом КС1.
5. При установке Java получить у производителя последнюю официальную версию, содержащую все программные обновления, связанные с безопасностью.
6. Перед установкой СКЗИ проверить программное обеспечение ПЭВМ на отсутствие вирусов и программных закладок.
7. Предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленной СКЗИ (путем опечатывания системного блока и разъемов ПЭВМ и контроля печатей администратором безопасности).
8. После установки «КриптоПро JCP» версия 2.0, но до начала его использования необходимо, воспользовавшись утилитой командной строки CPVerify.Prompt, создать хранилища контролируемых файлов, как описано в CPVerify.

17.1.Способы установки

Основной способ установки «КриптоПро JCP» версия 2.0 состоит в запуске командного файла, входящего в состав дистрибутива «КриптоПро JCP» версия 2.0, имя командного файла зависит от операционной системы, на которую производится установка. Другие варианты установки: использование установщика setup.exe и setup_console.bat (Windows) или setup_gui.sh и setup_console.sh (*nix или Mac OS).

Перед установкой «КриптоПро JCP» версия 2.0 необходимо предварительно удалить предыдущую версию продукта.

Для установки «КриптоПро JCP» версия 2.0 Вы должны иметь права администратора на данной рабочей станции.

17.2.Кодировки в Java

При запуске классов «КриптоПро JCP» версия 2.0 будет выводить сообщения в кодировке принятой в Вашей java по умолчанию. В случае несовпадения кодировки, установленной в java при запуске, и кодировки окна, прочитать текст будет невозможно. Изменить кодировку при запуске java можно указав значением переменной file.encoding нужную кодировку, например

```
java -Dfile.encoding=Cp866 -version
```

Из кода программы сменить кодировку можно методом

System.setProperty("file.encoding", "UTF-8");

Если Вы хотите, чтоб «КриптоПро JCP» версия 2.0 выводил сообщения в другой кодировке, измените значение переменной. Такое возможно, например, если Вы собираетесь перенаправить вывод в файл

setup_console.bat \java >log.txt 2>&1

и анализировать его потом используя другую кодировку.

В Unix-системах java-машины используют для определения кодировки значение переменной LANG. Следите за тем, чтобы значение этой переменной совпадало с кодировкой Вашего окна.

17.2.1.Установка на Windows

Установка «КриптоПро JCP» версия 2.0 должна проводится администратором из командной строки, находясь в папке с инсталлятором:

```
setup_console.bat <путь_к_JRE>,
```

например,

```
setup_console.bat "C:\Program Files\Java\jdk1.6\jre"
```

При этом будет использоваться исполняемый файл <JRE>\bin\java.exe, а также будет произведено полное удаление файлов «КриптоПро JCP» версия 2.0, что может быть необходимо при разрешении ошибочных ситуаций. В любом случае, перед установкой автоматически осуществляется попытка деинсталляции «КриптоПро JCP» версия 2.0 на случай, если оно было ранее установлено. Если имя компании содержит пробелы, то оно должно быть заключено в кавычки. Если имя компании указывается на русском языке, то кодировка должна совпадать с указанной в <JRE>\lib\font.properties

По окончании процесса установки необходимо убедиться в корректности установки и ввести лицензию (см. «Проверка и ввод лицензии»), если она не была указана сразу, для этого запустите файл:

```
ControlPane.bat <путь_к_JRE>
```

Если установка завершилась успешно, то будет запущена контрольная панель «КриптоПро JCP» версия 2.0. При необходимости введите лицензию, как это описано документе «ЖТЯИ.00091-01 91 02. Инструкция по использованию», раздел "Контрольная панель".

Удаление «КриптоПро JCP» версия 2.0 проводится администратором из командной строки:

```
setup_console.bat <путь_к_JRE>
```

При этом будет использоваться исполняемый файл <JRE>\bin\java.exe, а также будет произведено полное удаление файлов «КриптоПро JCP» версия 2.0.

В связи с возможностью одновременного сосуществования нескольких JRE на одной машине необходимо следить за тем, чтобы установка, удаление и использование «КриптоПро JCP» версия 2.0 проводилось одним и тем же JRE, то есть программные модули запускались одним и тем же файлом <JRE>\bin\java.exe.

Установка «КриптоПро JCP» версия 2.0 должна осуществляться администратором. На Windows Vista/2008/7/2008R2/8/2012/8.1/2012R2 запуск командного файла следует выполнять как "Run as administrator".

Другой вариант установки – использование приложения setup.exe <JRE>, осуществляющего запуск графического инсталлятора.

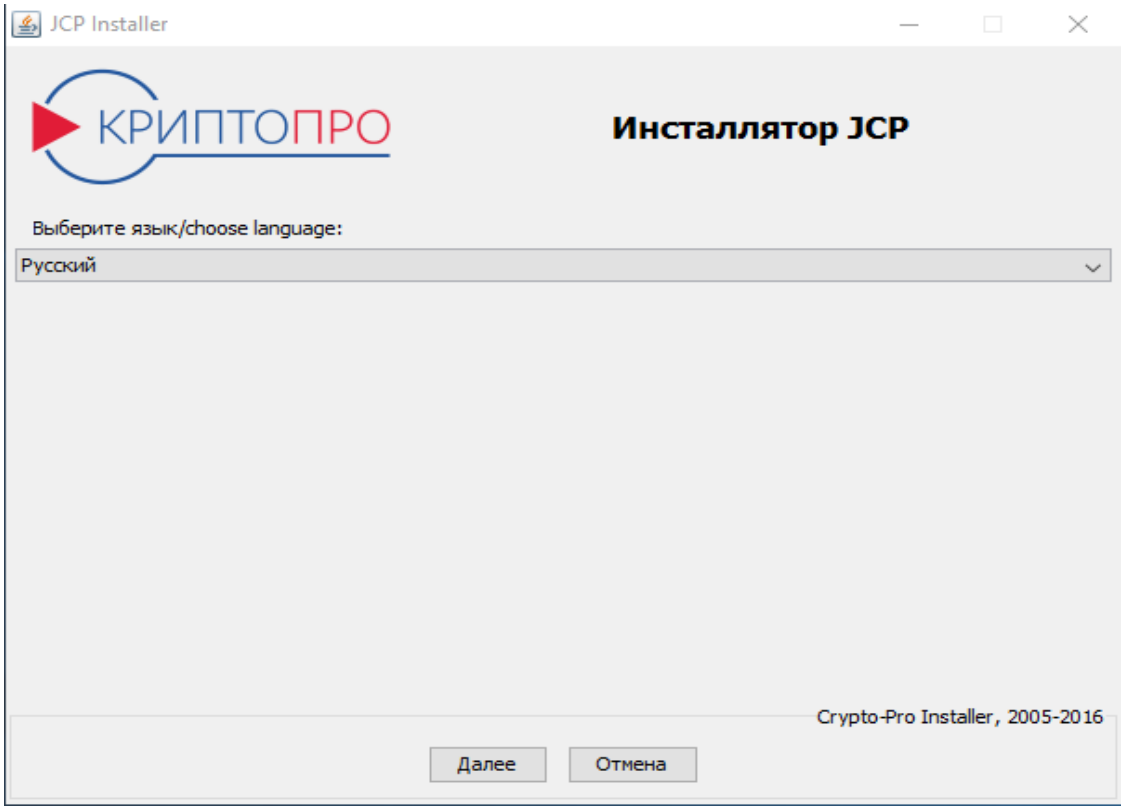

Рисунок 3. Выбор языка инсталлятора.

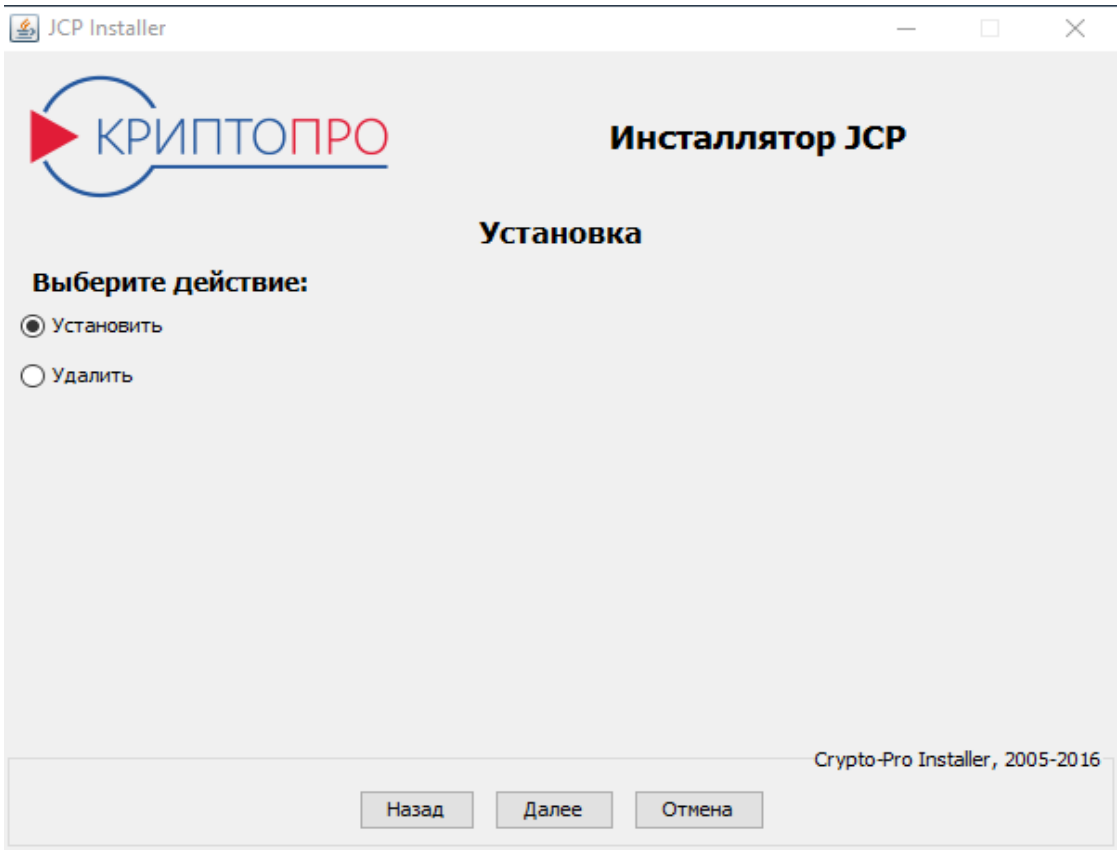

Рисунок 4. Выбор действия.

После выбора языка и действия (установка/удаление) будет предложено указать, в какой JRE будут производиться настройка, какие модули следует установить/удалить/обновить.

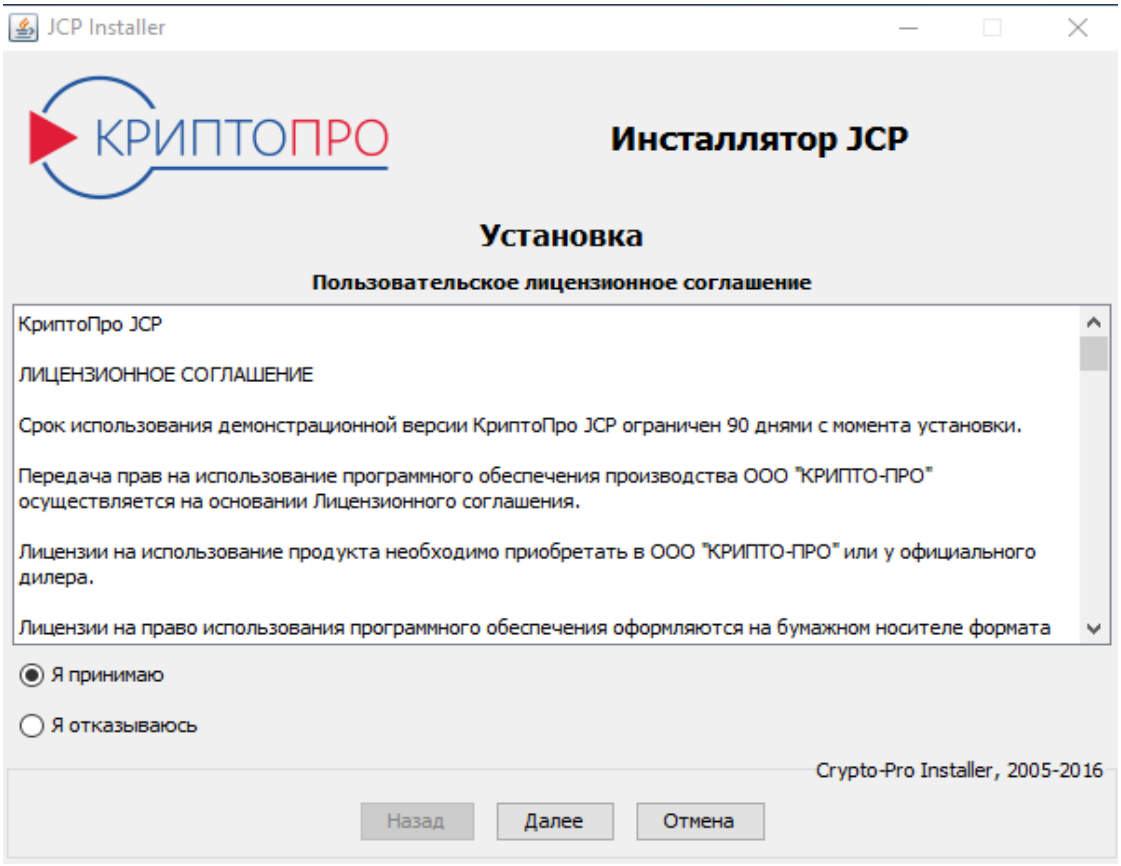

Рисунок 5. Лицензионное соглашение.

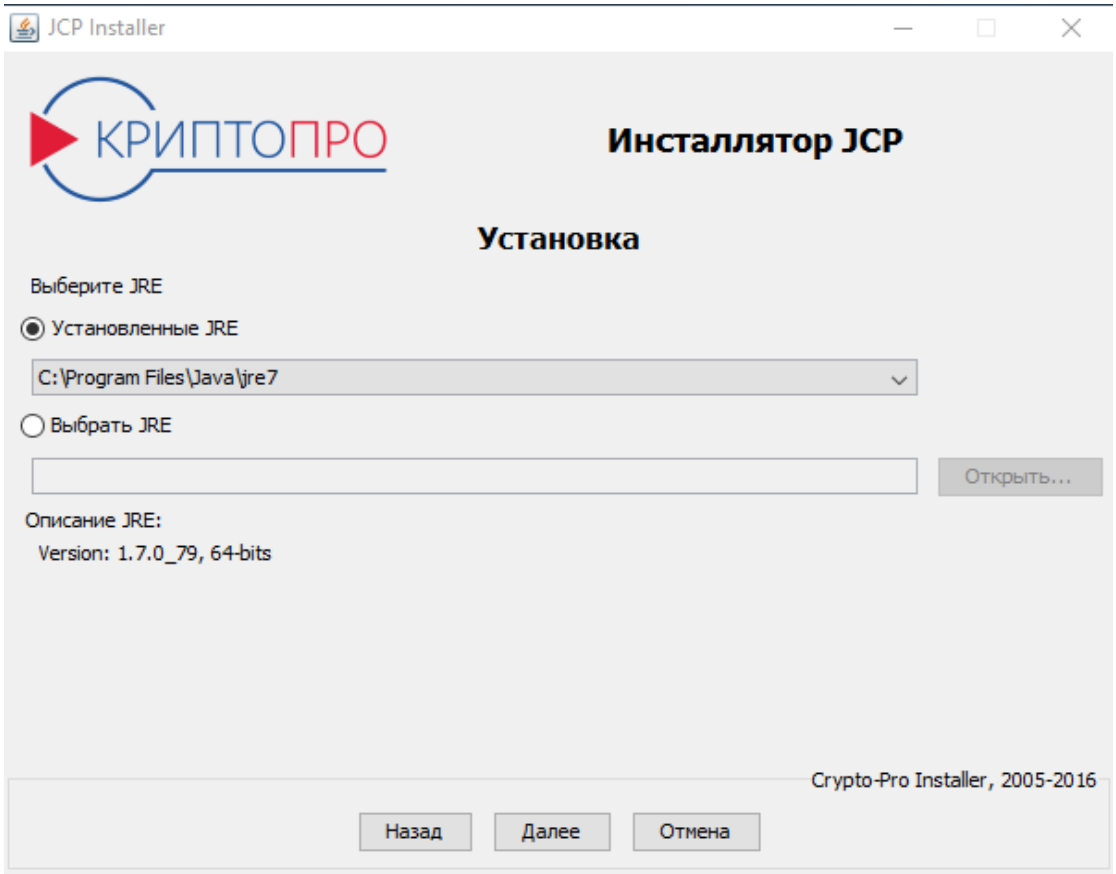

Рисунок 6. Выбор JRE.

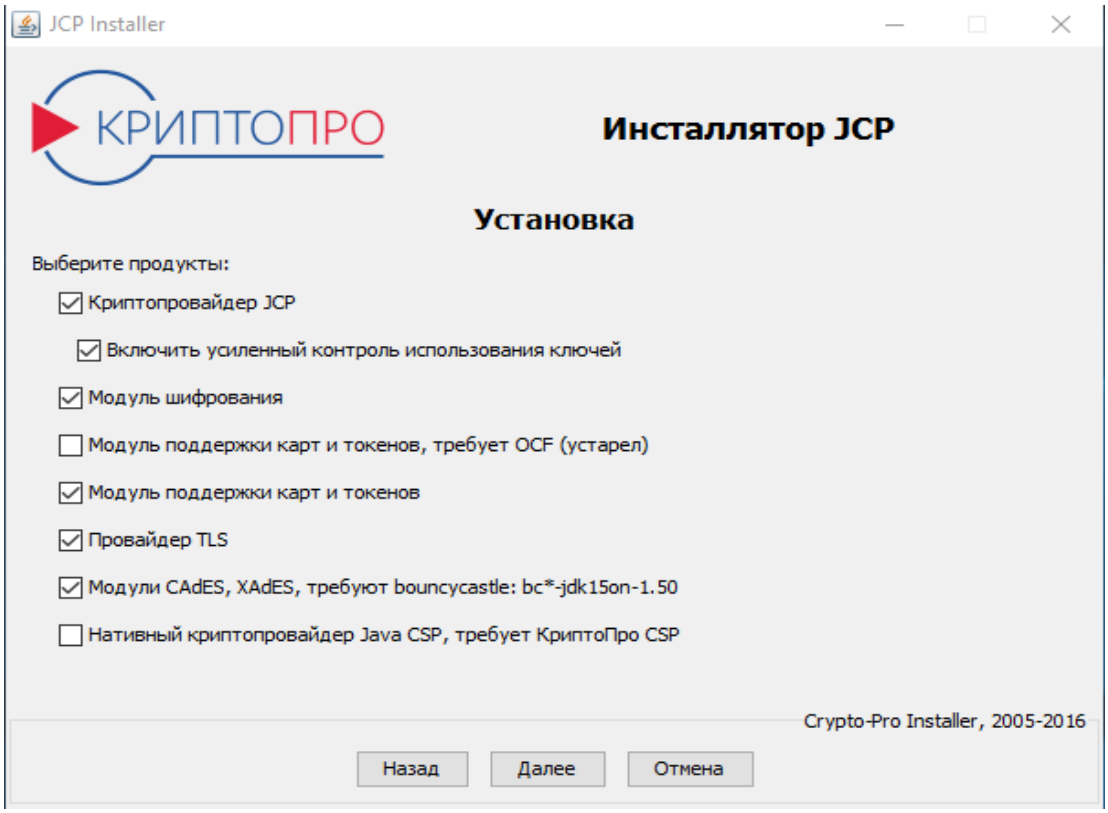

Рисунок 7. Выбор продуктов.

Внимание! При установке криптопровайдера «КриптоПро JCP» версия 2.0 необходимо **в обязательном порядке включить режим усиленного контроля использования ключей**. После установки при первом использовании СКЗИ для инициализации встроенных в СКЗИ ПДСЧ будет произведён запуск БиоДСЧ.

В случае, если режим усиленного контроля использования ключей не был включен при инсталляции СКЗИ, данный режим следует **в обязательном порядке** включить через контрольную панель СКЗИ. **Использование СКЗИ с выключенным режимом усиленного контроля использования ключей допускается исключительно в тестовых целях!**

С помощью пункта «Установить» может быть произведена как установка, так и обновление модулей. Если в указанной JRE уже имеется установленный «КриптоПро JCP» версия 2.0 и другие модули, то может быть предложено их обновить, если их версия устарела. Затем будет предложено указать серийные номера. Если они не указаны, то будут использованы серийные номера по умолчанию сроком действия 3 месяца. Тут же возможна проверка лицензий.

Важно! При установке модуля поддержки карт и токенов, требующего OCF, необходимо предварительно установить Open Card Framework. При установке модуля CadES необходимо скопировать в папку <JRE>/lib/ext файлы библиотек bouncycastle.

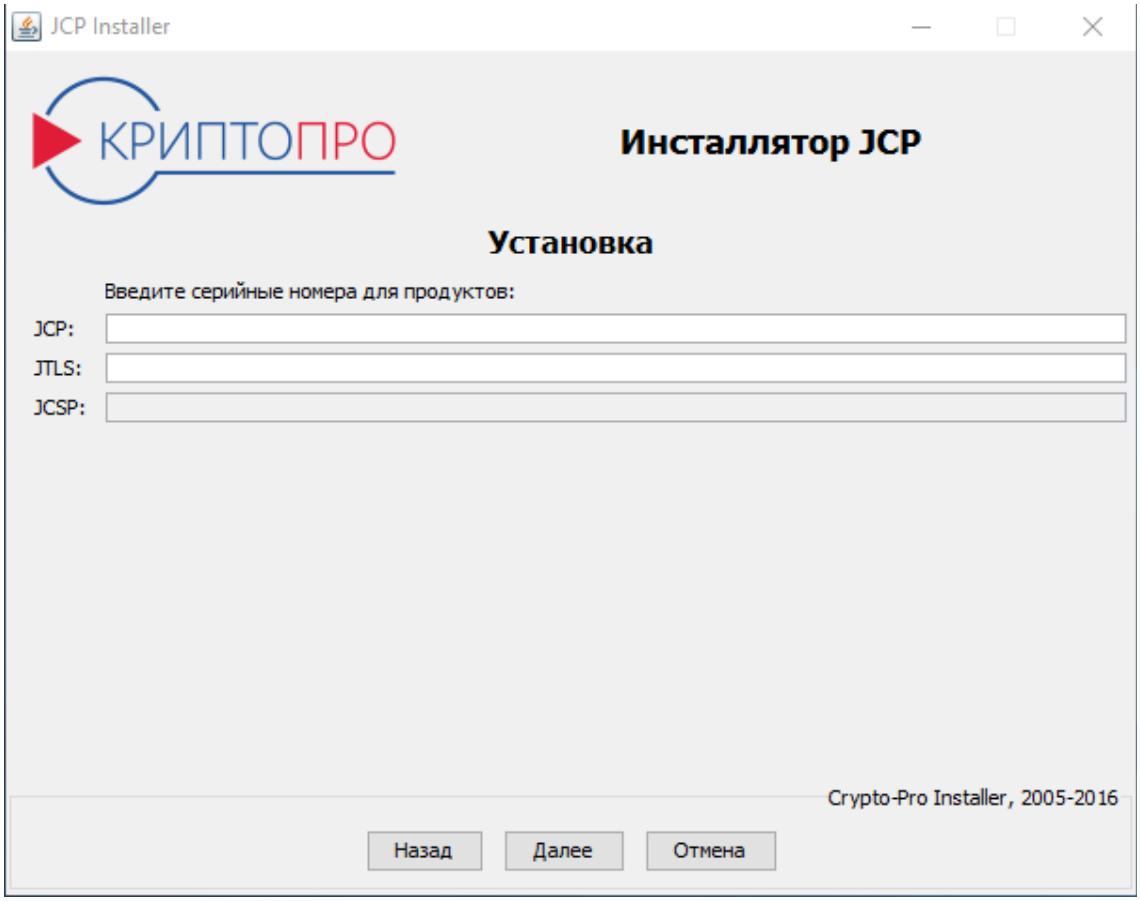

Рисунок 8. Ввод и проверка серийных номеров.

Далее будет предложено проверить корректность введенной ранее информации, удаление настроек (в случае удаления модулей).

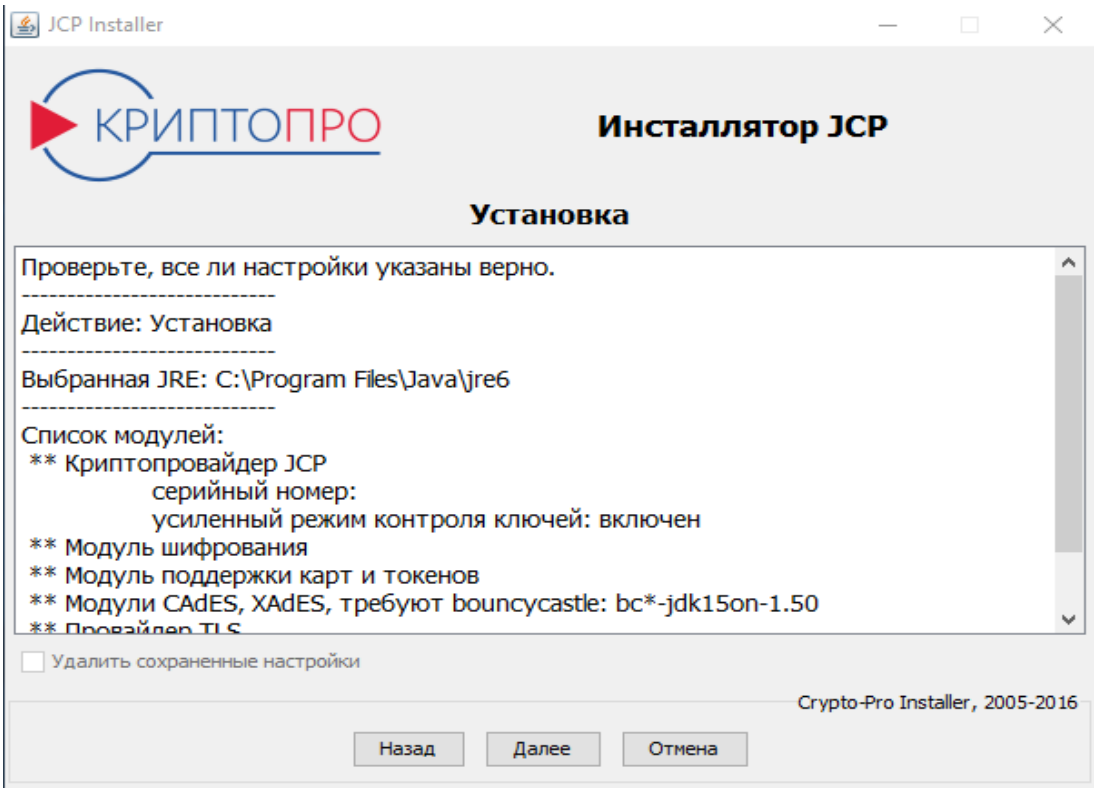

Рисунок 9. Проверка введенных данных.

Затем произойдет установка/удаление с выполнением логирования в окне установщика.

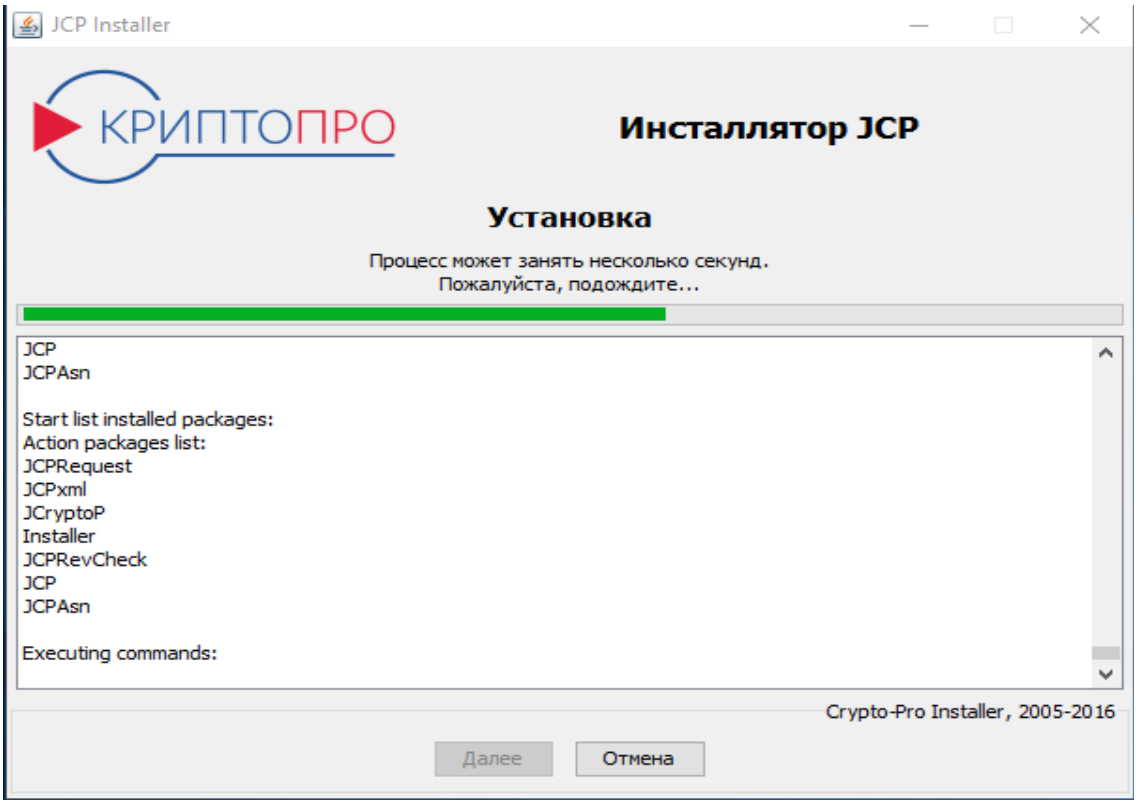

Рисунок 10. Выполнение операции.

В случае успешного выполнения будет отображено окно:

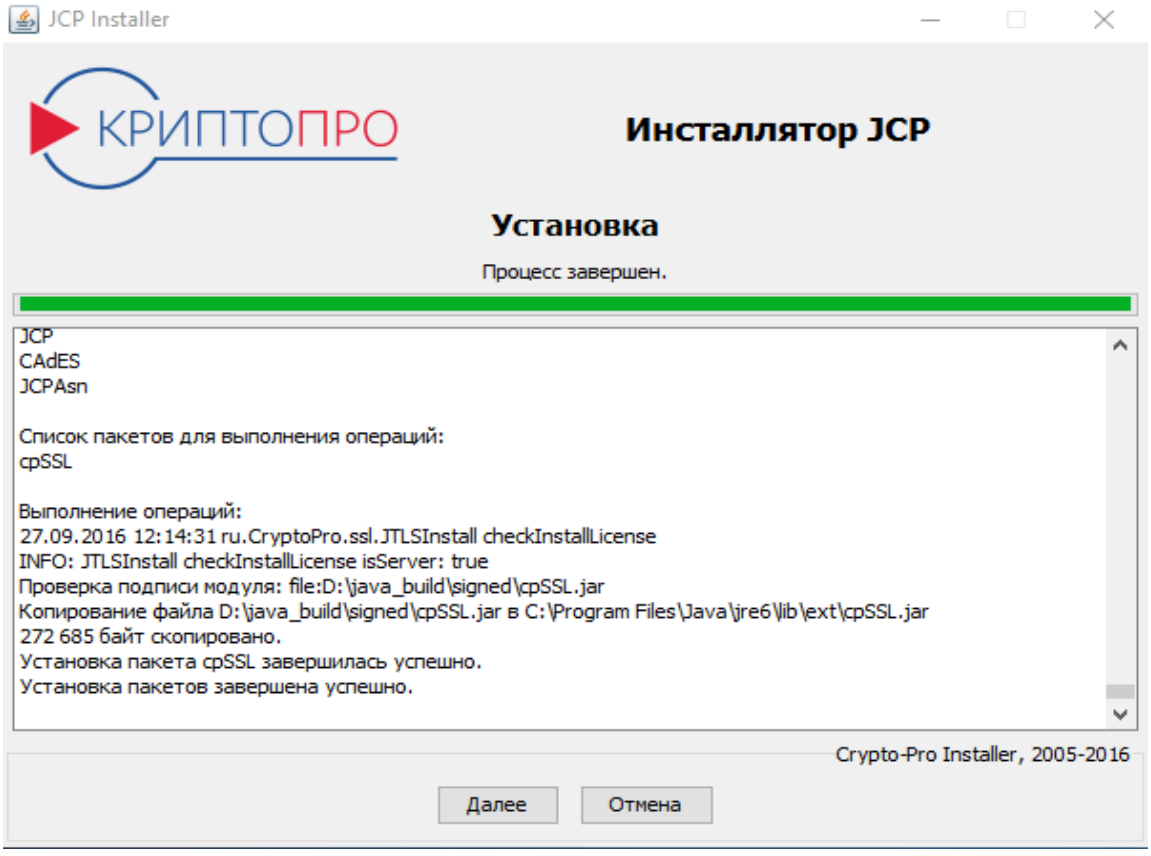

Рисунок 11. Завершение операции.

После перехода далее в случае установки может быть предложено запустить панель управления «КриптоПро JCP» версия 2.0.

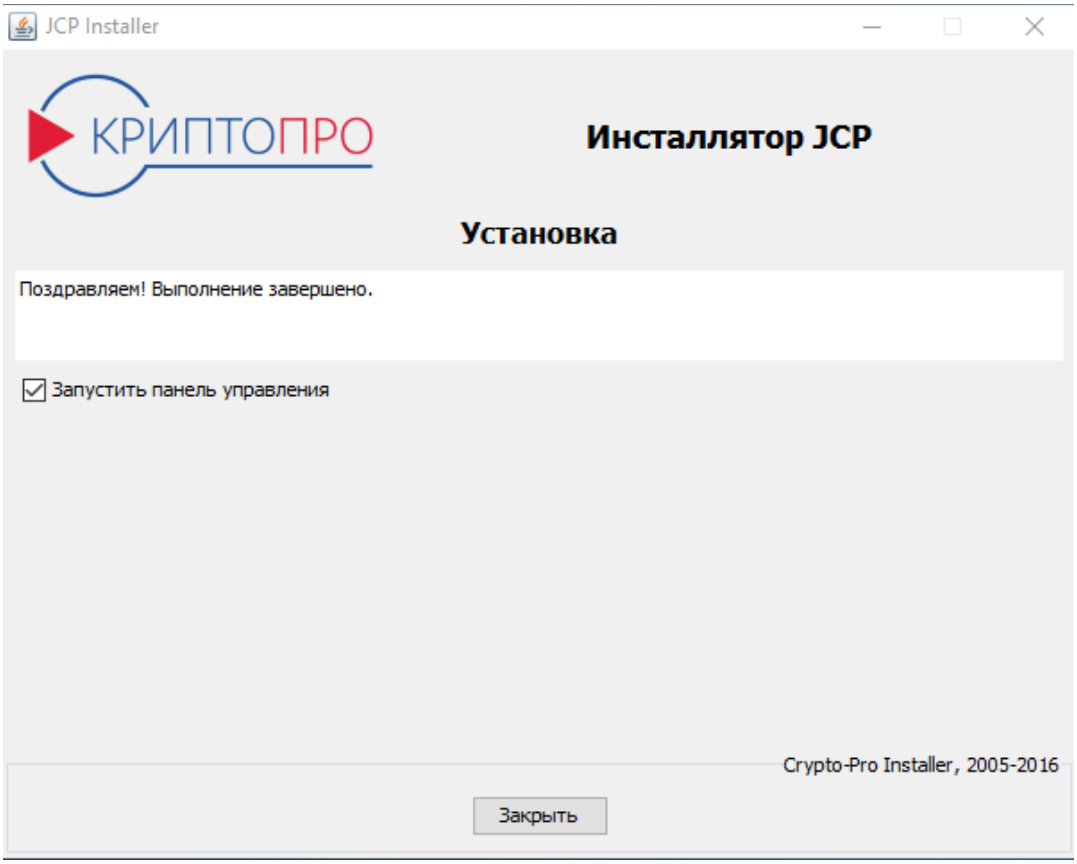

Рисунок 12. Успешное завершение и запуск панели.

Удаление отличается от установки только отсутствием некоторых шагов: лицензионное соглашение, ввод серийных номеров.

В случае ошибки соответствующее сообщение появится в ходе или при завершении операции.

Если по каким-то причинам удалить предыдущую версию «КриптоПро JCP» версия 2.0 не удается (например, файлы заняты другим процессом), будет предложено перезапустить инсталлятор.

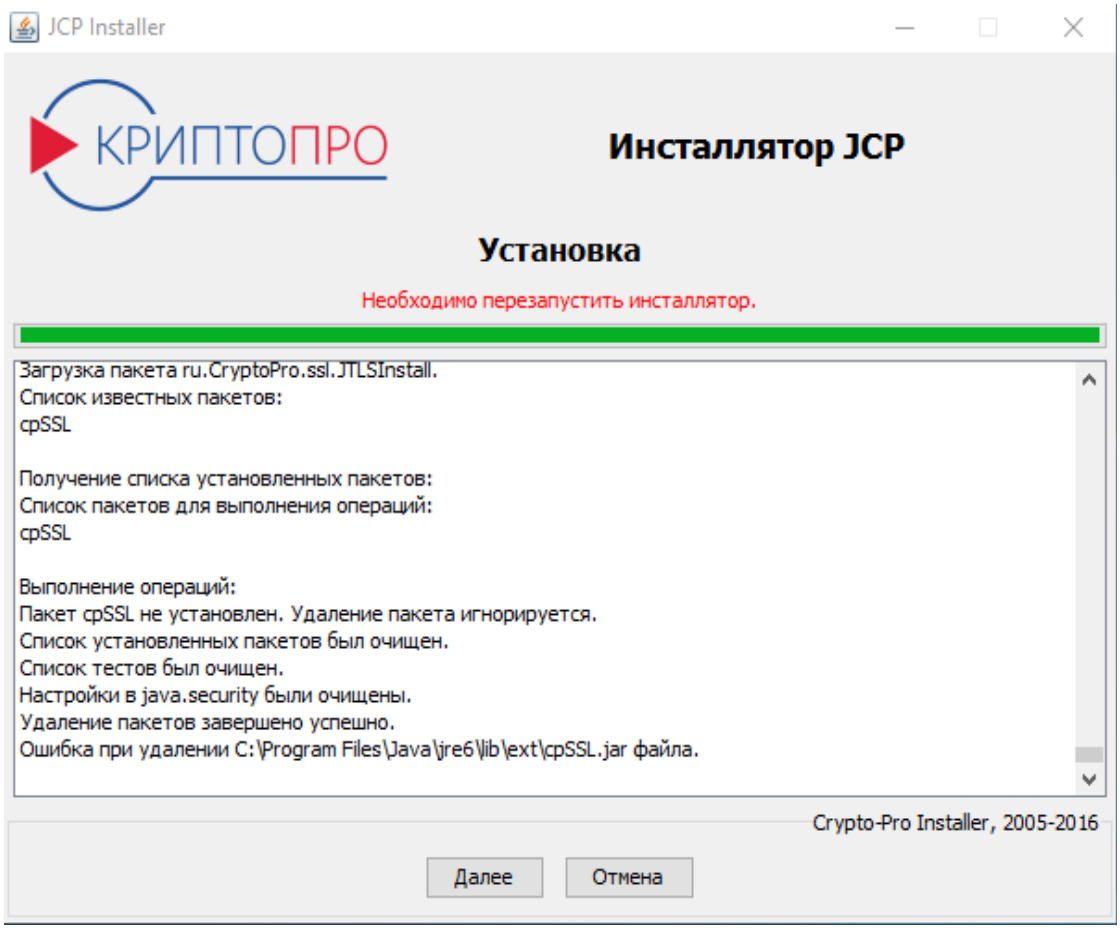

Рисунок 13. Перезапуск инсталлятора.

После нажатия на кнопку «Далее» инсталлятор будет перезапущен и перейдет к стадии проверки введенной информации (рис. 9), после чего ранее прерванная операция установки/удаления может быть возобновлена и завершена.

Консольная версия инсталлятора setup_console.bat при запуске требует указать JRE. Она мало отличается от графической версии. Возможны 2 варианта использования консольного инсталлятора:

а) пошагово указывать язык инсталлятора, JRE и вводить данные аналогично тому, как это делается в графическом инсталляторе; при этом можно использовать клавишу Enter для сохранения значения по умолчанию на каждом шаге.

б) выполнить установку/удаление без взаимодействия с пользователем. Обязательно необходимо указывать аргумент -force! Это возможно при использовании дополнительных параметров командной строки, например (setup_console.bat -help):

setup_console.bat <JRE> -force [-ru | -en] [-install | -uninstall] [-jre <value>] [-jcp | -jcryptop | -cpssl | -cades | -ocf | -j6cf | -cpssl | -jcsp] [-strict_mode] [-serial_jcp <value> -serial_cpssl <value> -serial_jcsp <value>] [-rmsetting]

где

•[-ru | -en] — язык инсталлятора,

•[-install | -uninstall] - выбранное действие (установка или удаление),

•[-jre <value>] - путь к JRE (по умолчанию, если параметр не задан, будет использоваться текущая исполняемая JRE),

•[-jcp | -jcryptop | -cpssl | -cades | -ocf | -j6cf | -cpssl | -jcsp] — основные доступные модули (jcp и модуль шифрования jcryptop образуют “Исполнение 2”, только один jcp – “Исполнение 1”),

•[-serial_jcp <value> -serial_cpssl <value> -serial_jcsp <value>] - серийные номера для выбранных продуктов,

• [-strict_mode] – включение режима усиленного контроля использования ключей (обязательно при инсталляции, потребует работы с БиоДСЧ),

•[-rmsetting] – удаление существующих настроек (только при удалении модулей).

Большинство аргументов может быть опущено. Так, отсутствие -jre приведет к использованию текущей исполняемой JRE, заданной в <JRE>.

Примеры команд:

1) установка «КриптоПро JCP» версия 2.0 (Вариант исполнения 2 — с модулем шифрования), cpSSL и CAdES в "C:\Program Files\Java\jre7" с указанием серийного номера для «КриптоПро JCP» версия 2.0.

setup_console.bat "C:\Program Files\Java\jre6" -force -ru -install -jre "C:\Program Files\Java\jre7" -jcp -jcryptop -cpssl -cades -serial_jcp XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

2) удаление «КриптоПро JCP» версия 2.0 в JRE по умолчанию (текущая исполняемая JRE) "C:\Program Files\Java\jre6".

setup_console.bat "C:\Program Files\Java\jre6" -force -en -uninstall -jcp

3) доустановк к уже установленному «КриптоПро JCP» версия 2.0 модуля Java CSP в JRE по умолчанию (текущая исполняемая JRE) с указанием серийного номера для Java CSP.

setup_console.bat "C:\Program Files\Java\jre6" -force -ru -install -jcsp -serial_jcsp XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

17.2.2.Установка на Unix и Mac OS

Установка «КриптоПро JCP» версия 2.0 на Unix осуществляется аналогично установке «КриптоПро JCP» версия 2.0 на Windows, с разницей лишь в исполняемых файлах для установки «КриптоПро JCP» версия 2.0, удаления «КриптоПро JCP» версия 2.0 и запуска контрольной панели «КриптоПро JCP» версия 2.0:

для установки «КриптоПро JCP» версия 2.0:

```
./setup_console .sh <путь_к_JRE> ,
```

например,

```
setup_console.sh /usr/java/jdk1.6/jre
```

для удаления «КриптоПро JCP» версия 2.0:

```
setup_console.sh <путь_к_JRE>
```

для запуска контрольной панели:

```
ControlPane.sh <путь_к_JRE>
```

При этом будет использоваться исполняемый файл <JRE>/bin/java.

Установка «КриптоПро JCP» версия 2.0 должна осуществляться администратором. Права, необходимые для установки «КриптоПро JCP» версия 2.0, можно получить:

1. Войти как пользователь root;
2. Выполнив команду "su";
3. Выполнив команду "sudo -s" (единственный штатный способ для Mac OS).

Другой вариант установки с помощью графического setup_gui.sh в системах Unix и Mac OS аналогичны Windows, за исключением одного отличия: JRE для установки/удаления в графическом инсталляторе необходимо указать с помощью кнопки «Открыть…» (рис. 6) или вписав в поле.

Графический инсталлятор запускается с помощью скрипта setup_gui.sh <JRE> под управлением учетной записи администратора.

17.2.3.Локальная установка вызовом Java

При установке «КриптоПро JCP» версия 2.0 на операционные системы отличные от Windows и Unix необходимо воспользоваться установкой через вызов программы java. Этот способ установки также может использоваться при частичной установке «КриптоПро JCP» версия 2.0, а также при установке из других программ.

Перед запуском установки необходимо убедиться в том, что:

- все файлы для установки находятся в одном каталоге;
- в переменной окружения PATH первым встречается каталог <JRE>/bin/ именно той java-машины, в которую планируется проводиться установка, либо при каждом выполнении команд указывается полный путь к исполняемому файлу java;
- установка производится администратором.

Для запуска программы установки необходимо вызвать java с именем jar файла, например:

```
java -classpath JCPinst.jar ru.CryptoPro.Install.VariantTwo
```

для установки Варианта 2 («КриптоПро JCP» версия 2.0 с функциями шифрования)

```
java -classpath JCPinst.jar ru.CryptoPro.Install.VariantOne
```

для установки Варианта 1 («КриптоПро JCP» версия 2.0 без функций шифрования)

Программа установки поддерживает следующие команды:

-install

Установка пакета или нескольких пакетов.

-uninstall

Удаление одного или нескольких пакетов.

-installed

Получение списка установленных пакетов.

-help

Получение справки.

При выполнении команды могут быть указаны дополнительные опции:

-skipFiles

Запретить копировать или удалять JAR-файлы.

-rmsetting

Удалить все настройки. При задании этой опции будут удалены все пользовательские и административные настройки. Рекомендуется использовать эту опцию только при полном удалении «КриптоПро JCP» версия 2.0 с компьютера. При переустановке «КриптоПро JCP» версия 2.0 на новую версию, эту опцию использовать не рекомендуется.

-verbose [<file>]

Детализированный вывод протокола на экран или в файл <file>.

-dest [<folder>]

Установить в каталог <folder>.

-force

Отключить проверку наличия ранее установленного/удаленного пакета.

Для полной установки «КриптоПро JCP» версия 2.0 в одном из стандартных исполнений необходимо запустить

```
java -classpath JCPinst.jar ru.CryptoPro.Install.VariantTwo -install
```

для установки Исполнения 2

```
java -classpath JCPinst.jar ru.CryptoPro.Install.VariantOne -install
```

для установки Исполнения 1.

Для выборочной первоначальной установки нескольких пакетов необходимо задать список устанавливаемых пакетов для опции install, например:

```
java -classpath JCPinst.jar ru.CryptoPro.Install.VariantOne -install Installer,JCP
```

Список возможных пакетов:

JCPinst

Пакет установки всех пакетов входящих в «КриптоПро JCP» версия 2.0 и «КриптоПро JTLS» версия 2.0, должен быть установлен.

JCP

Провайдер для подписи, должен быть установлен.

JCPControlPane

Панель для управления настройками, должен быть установлен.

ASN1P

Расширенный ASN, должен быть установлен.

OCF

Store для хранения ключей на смарт-картах, необязательный пакет, требует установки OpenCard Framework.

Oscar

Библиотека поддержки смарт-карты Оскар, необязательный пакет, необходим для хранения секретных ключей. Требует установки пакета OCF.

J6CF

Store для хранения ключей на смарт-картах, необязательный пакет, требует SUN java 1.6 (работа через пакет javax.smartcardio).

J6Oscar

Библиотека поддержки смарт-карты Оскар, необязательный пакет, необходим для хранения секретных ключей. Требует установки пакета J6CF.

JCPRequest

Пакет формирования запроса на сертификат, необязательный пакет, требует установки пакета ASN1P.

JCPxml

Пакет поддержки подписи xml в формате xmldsig, необязательный пакет.

JCryptoP

Криптопровайдер с функциями шифрования, необязательный пакет, входит только в Исполнение 2.

JCPRevCheck

Пакет поддержки совместимости с КриптоПро УЦ при проверке цепочки сертификатов, необязательный пакет, требует установки пакета ASN1P.

JCPRevCheck

Пакет со служебными классами для поддержки JCPRevCheck и JCPRequest, требует установки JCPRevCheck и JCPRequest.

cpSSL

Пакет реализующий протоколы SSL и TLS в соответствии с российскими криптографическими алгоритмами, необязательный пакет, не входит ни в одно из исполнений (устанавливается отдельно, см. «Руководство программиста» КриптоПро JTLS), требует установки пакетов JCP, ASN1P, JCryptoP.

При установке пакета JCP могут быть указаны дополнительные опции:

-serial XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Установка серийного номера XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

-company "Your Company"

Установка компании владельца серийного номера, используется только совместно с -serial. Если имя компании содержит пробелы, то оно должно быть заключено в кавычки.

Для удаления «КриптоПро JCP» версия 2.0 необходимо запустить класс вариант установки с опцией -uninstall, например следующим образом:

```
java ru.CryptoPro.Install.VariantTwo -uninstall -skipfiles delfiles.lst
```

После завершения процесса удаления «КриптоПро JCP» версия 2.0, необходимо удалить все файлы имена которых находятся в списке delfiles.lst.

Для частичного удаления «КриптоПро JCP» версия 2.0 (удаления нескольких пакетов) опции -uninstall можно задавать имена удаляемых пакетов аналогично опции -install. Так же при удалении можно задавать и другие опции, описанные выше.

Для получения списка установленных пакетов можно воспользоваться командной строкой:

```
java ru.CryptoPro.Install.VariantTwo –installed
```

17.2.4.Установка дополнительных пакетов

Установка дополнительных пакетов осуществляется другим способом. Для установки дополнительных пакетов, а так же пакетов входящих в состав «КриптоПро JCP» версия 2.0, но не установленных при начальной установке, необходимо использовать установщик входящий в состав дополнительного пакета или воспользоваться установкой пакета по умолчанию.

Установка дополнительного пакета с настройками по умолчанию, осуществляется вызовом java:

```
java –jar <имя jar>
```

Если пакет состоит из нескольких jar файлов, то все файлы пакета должны находится в одной директории. Удаление пакета можно проводить любым из способов описанных выше.

Установка дополнительного пакета с заданием опций, производится вызовом программы установки из этого пакета. Например:

```
java –classpath JCPxml.jar ru.CryptoPro.JCPxml.XMLInstall –install
```

Список опций класса установки совпадает со списком опций при установке из программы установки «КриптоПро JCP» версия 2.0. Ниже приведен полный список классов установки для всех пакетов входящих в «КриптоПро JCP» версия 2.0 и «КриптоПро JTLS» версия 2.0.

JCP

ru.CryptoPro.JCP.Install.JCPInstaller; установщик пакета находится в файле JCP.jar

ASN1P

ru.CryptoPro.JCP.Install.JCPAsnInstaller; установщик пакета находится в файле JCP.jar

OCF

ru.CryptoPro.JCP.KeyStore.OCF.Install; установщик пакета находится в файле OCF.jar

Oscar

ru.CryptoPro.JCP.KeyStore.Oscar.Installer; установщик пакета находится в файле Oscar.jar

J6CF

ru.CryptoPro.JCP.KeyStore.J6CF.Install; установщик пакета находится в файле J6CF.jar

J6Oscar

ru.CryptoPro.JCP.KeyStore.J6Oscar.Install; установщик пакета находится в файле J6Oscar.jar

JCPxml

ru.CryptoPro.JCPxml.XMLInstall; установщик пакета находится в файле JCPxml.jar

JCPRequest

ru.CryptoPro.JCPRequest.RequestInstall; установщик пакета находится в файле JCPRequest.jar

JCryptoP

ru.CryptoPro.Crypto.JCryptoPInstaller; установщик пакета находится в файле JCryptoP.jar

JCPRevCheck

ru.CryptoPro.reprov.Install; установщик пакета находится в файле JCPRevCheck.jar (также необходим JCPRevTools.jar)

cpSSL

ru.CryptoPro.ssl.JTLSInstall; установщик пакета находится в файле cpSSL.jar

AdES-core

ru.CryptoPro.AdES.installer.Install; установщик пакета находится в файле adES-core.jar

CAdES

ru.CryptoPro.CAdES.installer.Install; установщик пакета находится в файле CadES.jar

XadES

ru.CryptoPro.XAdES.installer.XAdESInstall; установщик пакета находится в файле XadES.jar

JCSP

ru.CryptoPro.JCSP.JCSPInstaller; установщик пакета находится в файле JCSP.jar

17.2.5.Проверка и ввод лицензии

Криптопровайдер «КриптоПро JCP» версия 2.0 имеет два типа лицензий: клиентские и серверные. Тип лицензии зависит от платформы, операционной системы и дальнейшего применения провайдера.

Клиентские ОС:

- Windows 2000 Proffesional;
- Windows XP;
- Windows Vista;
- Windows 7;
- Red Hat Enterprise Linux X.X Desktop;
- Red Hat Enterprise Linux X.X Workstation; (WS)
- Fedora X;
- SUSE Linux Enterprise Desktop XX;
- OpenSUSE Linux XX.X;
- Debian GNU/Linux X.X;
- Mandriva Corporate Desktop X;
- Ubuntu X.XX Desktop Edition;
- Linux XP Enterprise Desktop 2008;
- ALT Linux X.X Desktop;
- ALT Linux X.X Lite.

Серверные ОС:

- Windows 2000 Server;
- Windows 2003;
- Windows 2008;
- Solaris;
- FreeBSD;
- AIX;
- HP-UX;
- любые ОС на архитектуре отличной от ia32/amd64;

Если в дальнейшем предполагается использовать JTLS сервер, то необходима серверная лицензия «КриптоПро JCP» версия 2.0 (даже если по вышеуказанному списку подходит клиентская).

Для работы с лицензией можно использовать контрольную панель или командную строку (класс `ru.CryptoPro.JCP.tools.License`).

Минимальные требования к лицензии для данной системы указаны на контрольной панели (закладка "Общие"), также их можно узнать из командной строки:

```
ru.CryptoPro.JCP.tools.License -required
```

Ввод лицензии осуществляется через контрольную панель или вызовом класса `ru.CryptoPro.JCP.tools.License` с параметрами:

```
ru.CryptoPro.JCP.tools.License -serial "serial_number" -company "company_name" -store
```

или

```
ru.CryptoPro.JCP.tools.License -serial "serial_number" -combase "company_name_in_base64"
-store
```

Также можно проверить заданную лицензию без ее установки:

```
ru.CryptoPro.JCP.tools.License -serial "serial_number" -company "company_name"
```

или

```
ru.CryptoPro.JCP.tools.License -serial "serial_number" -combase "company_name_in_base64"
```

При использовании параметра "-combase" имя компании вводится в base64 кодировке.

Вызов класса `ru.CryptoPro.JCP.tools.License` без параметров проверит установленную лицензию.

Дату первой установки можно узнать с помощью команды:

```
ru.CryptoPro.JCP.tools.License -first
```

Для вывода справки:

```
ru.CryptoPro.JCP.tools.License ?
```

17.3.Установка модуля поддержки eToken

Для того чтобы использовать eToken как носитель ключевой информации для СКЗИ «КриптоПро JCP» версия 2.0 (тип хранилища "OCFStore" см. «Руководство программиста») в исполнительной среде Java Runtime Environment, необходимо выполнить следующие подготовительные действия:

- **Установить eToken RTE**;

Процедура установки подробно описана в руководстве пользователя eToken RTE

- **Установить исполнительную среду JRE**;
- **Установить OpenCard Framework** ;

OpenCard Framework (OCF) – это открытый стандарт, который обеспечивает поддержку смарт-карт на Java-платформе. eToken для «КриптоПро JCP» версия 2.0 использует OCF, поэтому следующим шагом будет установка библиотеки OCF.

Загрузите OCFbase и скопируйте все *.jar файлы в папку ${java.home}/jre/lib/ext, файлы *.properties в папку ${java.home}/jre/lib.

- **Установить «КриптоПро JCP» версия 2.0** (см. «Способы установки»);

Если JCP уже был установлен, его следует переустановить.

- **Установить модуль поддержки eToken для «КриптоПро JCP» версия 2.0**.

Модуль поддержки eToken для «КриптоПро JCP» версия 2.0 (также как и сам электронный ключ eToken) является продуктом компании Aladdin.
По всем вопросам использования обращаться к компании-разработчику.

Для установки программного обеспечения вы должны иметь права администратора на данной рабочей станции.

17.4.Установка модуля поддержки Rutoken

Для того чтобы использовать Rutoken как носитель ключевой информации для СКЗИ «КриптоПро JCP» версия 2.0 в исполнительной среде Java Runtime Environment, необходимо выполнить следующие подготовительные действия:

- Установить драйверы Rutoken;
- Установить исполнительную среду JRE;
- Установить «КриптоПро JCP» версия 2.0 (см. «Способы установки»);

Если «КриптоПро JCP» версия 2.0 уже был установлен, его следует переустановить.

- Установить модуль поддержки Rutoken для «КриптоПро JCP» версия 2.0.

Модуль поддержки Rutoken для «КриптоПро JCP» версия 2.0 (также как и сам электронный ключ Rutoken) является продуктом компании Рутокен.

По всем вопросам использования обращаться к компании-разработчику.

17.5.Политики безопасности

${java.home}/lib/security/java.policy

17.5.1.Права доступа для JCP.jar

«КриптоПро JCP» версия 2.0 устанавливается в каталог `${java.home}\lib\ext`. Обычно этот каталог имеет права доступа разрешающие всем jar файлам, содержащимся в этом каталоге, получить все права доступа

```
grant codeBase "file:${java.home}/lib/ext/*" {
    permission java.security.AllPermission;
};
```

Если этот каталог имеет права доступа отличные от приведенных выше необходимо настроить права доступа для JCP.jar. Примерный вид этого файла приведен ниже.

```
grant codeBase "file:${java.home}/lib/ext/jcp.jar" {
    permission java.lang.RuntimePermission "preferences", "read";
    permission java.util.PropertyPermission "os.name", "read";
    java.util.PropertyPermission "<usedProperty>", "read";
    permission java.io.FilePermission "<pathToLocalMutex>/*" "read, write";
};
```

где

- **<usedProperty>** - Property используемые при настройке, каких-либо путей.
- **<pathToLocalMutex>** Путь к UnixMutex для пользователя (подробнее см. «Настройки контрольной панели»)

17.5.2.Права доступа для администратора JCP

Администратору безопасности должны быть предоставлены следующие права доступа:

```
grant {
    permission java.lang.RuntimePermission "preferences", "read";
}
```

Кроме того, администратор безопасности должен иметь:

- права доступа зависящие от операционной системы для доступа к настройкам Preferences. Например, для Windows администратор безопасности должен иметь права доступа для чтения/записи в ключ реестра `HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\ru\/Crypto/Pro\/J/C/P`

17.5.3.Права доступа для приложений

Установленные на JAVA машину приложения не должны осуществлять доступ к ключам. Для этого все приложения установленные на Java машину должны быть или получены от производителей доверенным способом или иметь права доступа запрещающие доступ к ключам.

Обычно каталог `${java.home}\lib\ext` разрешает всем приложениям для всех пользователям все права доступа. Необходимо или ограничить эти права доступа,

запретив доступ в каталоги содержащие ключи (а так же к смарт-карте и дискете) или устанавливать в этот каталог только приложения производителей полученные доверенным способом.

17.5.4.Права доступа пользователя

Пользователь «КриптоПро JCP» версия 2.0 должен обладать следующими правами доступа:

- Права доступа, зависящие от операционной системы, для доступа к настройкам Preferences. Например, для Windows пользователь должен иметь права доступа для чтения из ключа реестра `HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\ru\/Crypto/Pro\/J/C/P;`

- Права доступа, зависящие от операционной системы, на чтения/запись файлов во временный каталог (см. настройки контрольной панели);

- Права доступа, зависящие от операционной системы, на чтение/записи/создание каталогов в файлы ключей (см. настройки контрольной панели)

- Права доступа, зависящие от операционной системы, на чтение/запись/создание каталогов на дискету (при использовании носителя дискета)

Примечание: для Unix платформ папки `keys` и `tmp`, заданные по умолчанию (`/var/cprocsp/keys` и `/var/cprocsp/tmp`), могут быть созданы только из под root. Для их автоматического создания с правильными правами доступа достаточно создать контейнер из под root.

18.Управление протоколами

Журналирование «КриптоПро JCP» версия 2.0 осуществляется стандартными средствами Java машины. Формат протокола, поля вывода, уровни протоколирования настраивается в файле **<jre>/lib/logging.properties**. Имя класса протокола для JCP: **ru.CryptoPro.JCP.tools.JCPLogger**.

Уровни протоколирования «КриптоПро JCP» версия 2.0 совпадают с уровнями протоколирования Java, ниже они приведены в порядке по возрастанию информативности сообщений, уровень выше включает все сообщения приведенные по тексту ниже. Уровень **ALL** включает все сообщения, уровень **OFF** выключает все сообщения.

При настройках Java машины по умолчанию, включен уровень **INFO**.

- **OFF** В протокол не выводятся никакие сообщения.
- **SEVERE** - Критические ошибки в «КриптоПро JCP» версия 2.0, функционирование «КриптоПро JCP» версия 2.0 после появления этих ошибок невозможно. К ним относятся ошибки загрузки, ошибки контроля целостности и др.
- **WARNING** - Ошибки «КриптоПро JCP» версия 2.0. Ошибки не приводящие к отказу функционирования «КриптоПро JCP» версия 2.0. К ним относятся, например ошибки настройки «КриптоПро JCP» версия 2.0, неправильный вызов функций «КриптоПро JCP» версия 2.0.
- **INFO** - Информационные сообщения о загрузке «КриптоПро JCP» версия 2.0.
- **CONFIG** - Информационные сообщения при получении текущих настроек используемых «КриптоПро JCP» версия 2.0.
- **FINE** - Информационные сообщения о завершении функции провайдера с ошибкой.
- **FINER** - Информационные сообщения связанные с входом/выходом в/из функции провайдера.
- **FINEST** - Уровень, не используется
- **ALL** - Сам уровень не используется, приводит к выдаче всех сообщений выдаваемых «КриптоПро JCP» версия 2.0.

При включении уровня отличного от заданного по умолчанию (**INFO**) следует помнить, что уровни выше **CONFIG** могут значительно замедлить скорость провайдера, а уровни ниже **INFO** привести к несвоевременному обнаружению причин отказа «КриптоПро JCP» версия 2.0. При обычной работе «КриптоПро JCP» версия 2.0 рекомендуется оставлять настройку уровня выводимых сообщений по умолчанию (**INFO**).

Пример настройки файла logging.properties с уровнем FINE (исправления выделены жирным):

```
...
# Default global logging level.
# This specifies which kinds of events are logged across
# all loggers.  For any given facility this global level
# can be overriden by a facility specific level
# Note that the ConsoleHandler also has a separate level
# setting to limit messages printed to the console.
.level= INFO

############################################################
# Handler specific properties.
# Describes specific configuration info for Handlers.
############################################################

# default file output is in user's home directory.
java.util.logging.FileHandler.pattern = %h/java%u.log
```

```
java.util.logging.FileHandler.limit = 50000
java.util.logging.FileHandler.count = 1
java.util.logging.FileHandler.formatter = java.util.logging.XMLFormatter

# Limit the message that are printed on the console to INFO and above.

#java.util.logging.ConsoleHandler.level = INFO
java.util.logging.ConsoleHandler.level = FINE
java.util.logging.ConsoleHandler.formatter = java.util.logging.SimpleFormatter

############################################################
# Facility specific properties.
# Provides extra control for each logger.
############################################################

# For example, set the com.xyz.foo logger to only log SEVERE
# messages:

com.xyz.foo.level = SEVERE

ru.CryptoPro.JCP.tools.JCPLogger.level = FINE
...
```

19.Требования по защите от НСД

19.1.Принципы защиты информации от НСД

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

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

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

Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или контролирующими органами.

В организации, эксплуатирующей ПО СКЗИ «КриптоПро JCP» версия 2.0, должна быть выпущена инструкция по защите от НСД к системе, разработанная на базе настоящего документа, руководящих документов Государственной технической комиссии, действующих нормативных документов самой эксплуатирующей организации.

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

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

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

При осуществлении доступа в глобальные сети передачи данных непосредственно с рабочих мест, оснащенных СКЗИ «КриптоПро JCP» версия 2.0, должны быть приняты меры, исключающие возможность воздействия нарушителя на СКЗИ по каналам связи, выходящим за пределы контролируемой зоны.

19.2.Меры по обеспечению защиты информации от НСД

- При использовании СКЗИ «КриптоПро JCP» версия 2.0 необходимо наличие механизма локальной аутентификации пользователей ОС;

- Необходимо разработать и применить политику назначения и смены паролей в соответствии со следующими правилами:

- Длина пароля должна быть не менее 8 символов;

- Количество подряд следующих попыток аутентификации одного субъекта доступа должно быть не более 10. При превышении числа подряд идущих попыток аутентификации одного субъекта доступа установленного предельного значения доступ этого субъекта к СКЗИ блокируется на сутки;

- Недопустимо при выборе каждого символа пароля ограничиваться менее, чем 10 вариантами;

- Периодичность смены пароля не должна превышать 6 месяцев.

Для обеспечения требований к установлению пароля должны выполняться следующие настройки операционных систем:

Linux:

В файле /etc/login.defs параметр LOGIN_RETRIES не должен превышать 10
PASS_MAX_DAYS=180
В файле небходимо добавить опцию min /etc/pam.d/common-password:
password [success=1 default=ignore] pam_unix.so obscure sha512 min=10

AIX:
В файле /etc/security/user
в секции default необходимо установить следующие значения:
minlen = 6
maxrepeats = 10
maxage=24

Solaris:
В файле /etc/default/passwd необходимо установить следующие значения
PASSLENGTH=6
MAXREPEATS=10
MAXWEEKS=24

Windows:

В групповых политиках перейти в
Local Computer Policy->Computer Configuretion->Windows Settings->SecuritySettings->Account Policies
В Account Policies установить следующие параметры:

Minimum password length = 6
Maximum password age = 24

Перейти в
Local Computer Policy->Computer Configuretion->Windows Settings->SecuritySettings->Account Lockout Policies
Установить параметр

Account Lockout threshold = 10

При использовании СКЗИ «КриптоПро JCP» версия 2.0 также следует принять следующие организационные меры:

1. Провайдер «КриптоПро JCP» версия 2.0 должен использоваться в среде, защищенной от действий внешнего нарушителя, и в корпоративных сетях, защищенных от внутреннего нарушителя.
2. Необходимо ограничить возможность вывода информации с используемой ПЭВМ через порты COM, LPT, USB, IEEE 1394, а также средствами Bluetooth, Wi-Fi и аналогичных.
3. Право доступа к рабочим местам с установленным ПО СКЗИ «КриптоПро JCP» версия 2.0 предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе СКЗИ «КриптоПро JCP» версия 2.0.
4. Запретить осуществление несанкционированного администратором безопасности копирование ключевых носителей.
5. Запретить разглашение содержимого ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер.
6. Запретить использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ «КриптоПро JCP» версия 2.0, либо использовать ключевые носители на посторонних ПЭВМ.
7. Запретить запись на ключевые носители посторонней информации.
8. Требования по хранению личных ключевых носителей распространяются на ПЭВМ (в том числе и после удаления ключей с диска).
9. На технических средствах, оснащенных СКЗИ «КриптоПро JCP» версия 2.0, должно использоваться только лицензионное программное обеспечение фирм-производителей.
10. На ПЭВМ, оснащенных СКЗИ «КриптоПро JCP» версия 2.0, не допускается установка средств разработки и отладки ПО. Если средства отладки приложений необходимы для технологических потребностей пользователя, то их использование должно быть санкционировано администратором безопасности.

В любом случае запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений, использующих СКЗИ «КриптоПро JCP» версия 2.0. Необходимо исключить попадание в систему программ, позволяющих, пользуясь ошибками ОС, получать привилегии администратора.

11. Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства СКЗИ «КриптоПро JCP» версия 2.0, по роду своей деятельности не являющихся персоналом, допущенным к работе в указанных помещениях.

12. Должно быть запрещено оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ «КриптоПро JCP» версия 2.0 после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

13. Администратором безопасности должно быть проведено опечатывание системного блока с установленным СКЗИ «КриптоПро JCP» версия 2.0, исключающее возможность несанкционированного изменения аппаратной части рабочей станции.

14. Из состава системы должно быть исключено все оборудование, которое может создавать угрозу безопасности ОС. Также избегают использования любых нестандартных аппаратных средств, имеющих возможность влиять на нормальный ход работы компьютера или ОС.

15. При использовании СКЗИ «КриптоПро JCP» версия 2.0 на ПЭВМ, подключенных к общедоступным сетям связи, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей.

16. В BIOS ПЭВМ определяются установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС.

17. Средствами BIOS должна быть исключена возможность отключения пользователями ISA и PCI устройств при использовании ПАК защиты от НСД, устанавливаемых в ISA и PCI разъем.

18. Вход в BIOS ПЭВМ должен быть защищен паролем, к которому предъявляются те же требования, что и к паролю администратора. Пароль для входа в BIOS должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС.

19. Средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты.

20. При загрузке ОС должен быть реализован контроль целостности программного обеспечения, входящего в состав СКЗИ «КриптоПро JCP» версия 2.0, самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ.

21. Должно быть реализовано физическое затирание содержимого удаляемых файлов, в том числе SWAP файла.

22. Должно быть обеспечено тестирование аппаратуры в обьеме самотестирования при перезагрузке не реже чем 1 раз в 15 суток.

23. Переставлять реализацию класса Preferences с помощью property java.util.prefs.PreferencesFactory запрещается.

24. Необходимо обеспечить административными мерами контроль доступа к системным и пользовательским настройкам Java-машины.

При использовании «КриптоПро JCP» версия 2.0 на платформе Windows Java-машина системные и пользовательские настройки хранит в реестре в разделах HKEY_CURRENT_USER\Software\JavaSoft\Prefs и HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs соответсвенно.

На платформах Solaris и Linux Java-машина системные и пользовательские настройки хранит в файловой системе. Системные настройки находятся в каталоге .systemPrefs, положение которого определяется переменной java.util.prefs.systemRoot (по умолчанию /etc/.java). Если он недоступен то .systemPrefs находится в каталоге определенном переменной java.home

Пользовательские настройки находятся в каталоге .java/.userPrefs, положение которого определяется переменной java.util.prefs.userRoot. Если переменная не задана то каталог .java/.userPrefs находится в каталоге определенном переменной user.home.

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

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

1. Использование шифровальных средств для криптографической защиты информации подлежит лицензированию в соответствии с действующим законодательством РФ.
2. Рабочие места, на которые установлены СКЗИ, должны быть аттестованы комиссией. Результаты работы комиссии отражаются в Акте готовности к работе.
3. Правом доступа к рабочим местам с установленным СКЗИ должны обладать только лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, использующего СКЗИ, с правилами пользования или с другими нормативными документами, созданными на их основе.
4. Должностные инструкции администратора безопасности (его заместителя) и ответственного исполнителя должны учитывать требования настоящих Правил.
5. При каждом включении рабочей станции с установленным СКЗИ необходимо проверять сохранность печатей системного блока и разъемов рабочей станции.
6. Администратор безопасности должен периодически (не реже 1 раза в 2 месяца) проводить контроль целостности и легальности установленных копий ПО на всех АРМ со встроенной СКЗИ с помощью программ контроля целостности.
7. В случае обнаружения "посторонних" (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией в составе представителей служб информационной безопасности организации - владельца сети и организации - абонента сети, где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения.
8. Не допускается оставлять без контроля вычислительные средства, входящие в состав СКЗИ, при включенном питании и загруженном программном обеспечении СКЗИ. При кратковременном перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана производится с использованием пароля доступа.
9. Пользователь должен запускать только те приложения, которые разрешены администратором безопасности.
10. Средствами BIOS должна быть исключена возможность отключения пользователями ISA-устройств.
11. ПО, установленное на ПЭВМ, не должно иметь встроенных средств разработки и отладки программ.
12. ПЭВМ, обеспечивающие удаленный вход пользователей из глобальной сети, не должны использовать ПО СКЗИ.
13. Пароли, назначаемые пользователям, должны отвечать требованиям соответствующих инструкции и нормативных документов.

Не допускается:

1. Осуществлять несанкционированное копирование ключевых носителей.
2. Разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер (за исключением случаев, предусмотренных данными правилами).
3. Вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя.
4. Подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией.
5. Работать на компьютере, если во время его начальной загрузки не проходит встроенный тест ОЗУ, предусмотренный в ПЭВМ.
6. Вносить какие-либо изменения в программное обеспечение СКЗИ.
7. Изменять настройки, установленные программой установки СКЗИ или администратором.
8. Использовать синхропосылки, вырабатываемые не средствами СКЗИ.
9. Обрабатывать на ПЭВМ, оснащенной СКЗИ, информацию, содержащую государственную тайну.

10. Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ «КриптоПро JCP» версия 2.0.

11. Осуществлять несанкционированное вскрытие системных блоков ПЭВМ.

12. Приносить и использовать в помещении, где размещены средства СКЗИ, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер).

21.Контроль целостности JAR файлов

Контроль целостности JAR-файла провайдера осуществляется при загрузке провайдера посредством проверки подписей трех файлов `JCP.jar`, `ASN1P.jar` и `asn1rt.jar`. Создание и проверка подписей JAR-файлов реализованы в классе `JarChecker`.

21.1.Создание подписи JAR-файла

Для создания подписи некоторого JAR-файла следует вызвать функцию *main* класса `JarChecker` со следующими параметрами:

```
-sign   [-alias keyAlias]  [-storetype storeType]  [-keypass keyPassword]
        [-in jar_file]  [-out signed_jar_file] [-delsign]
```

Описание передаваемых параметров:

параметр	значение	обязательный/необязательный
-sign	команда создания новой подписи	обязательный параметр
-alias	имя ключа электронной подписи, на котором осуществляется подпись	обязательный параметр
-storetype	имя ключевого носителя, на котором лежит ключ	по умолчанию - HDImageStore, обязательный если ключ лежит не на жестком диске
-keypass	пароль на ключ подписи	обязательный, если пароль на ключ установлен
-in	полный путь к подписываемому JAR-файлу	обязательный параметр
-out	полный путь к файлу, в который будет записан подписанный JAR-файл	обязательный параметр
-delsign	флаг, определяющий удаление неверных подписей	если указан, то неверные подписи будут удалены

Описание процесса создания подписи:

- в первую очередь осуществляется проверка всех существующих подписей;
- если существуют неверные подписи и указан параметр -delsign, то эти подписи удаляются;
- если после проверки и, возможно, удаления неверных подписей, общее количество подписей равно и превышает 16, то новая подпись создаваться не будет;
- если среди оставшихся подписей уже существует подпись на заданном ключе электронной подписи и она верна, то новая подпись не создается;
- если среди оставшихся подписей уже существует подпись на заданном ключе электронной подписи и она не верна, то неверная подпись удаляется (в независимости от флага -delsign) и создается новая подпись на этом ключе;
- в противном случае просто формируется новая подпись:

В процессе формирования подписи JAR-файла осуществляется копирование всех классов, входящих в исходный JAR-файл, в новый JAR-файл, определенный путем `-out`. После чего в директории META-INF нового JAR-файла создаются два файла: Digest.CP и Sign.CP (если подпись производится не в первый раз, т.е. если такие файлы уже существуют в исходном JAR-файле, то файл Digest.CP не изменяется, а к содержимому Sign.CP добавляется информация о новой подписи).

Первый файл представляется собой набор пар: имя класса, входящего в JAR-файл, но не входящего в директорию META-INF, и значение хэша на содержимое этого класса. Второй файл содержит в себе следующую информацию:

- количество подписей (уже существующих + только что созданная);
- набор подписей (уже существующие + новая подпись);
- набор соответствующих подписям сертификатов (уже существующие + новый).

Новая подпись (как и все предыдущие) производится на содержимое файла Digest.CP.

21.2. Проверка подписи JAR-файла

Для проверки подписи некоторого JAR-файла следует вызвать функцию *main* класса `JarChecker` со следующими параметрами:

```
-verify  [-in signed_jar_file] [-cert cert_file]
```

Описание передаваемых параметров:

параметр	значение	обязательный/необязательный
-verify	команда проверки подписи	обязательный параметр
-in	полный путь к подписанному JAR-файлу	обязательный параметр
-cert	полный путь к сертификату, на котором осуществляется проверка подписи	если указан, то осуществляет проверка подписи, соответствующей заданному сертификату. В противном случае осуществляется проверка всех имеющихся подписей JAR-файла

Описание процесса проверки подписи:

- если в JAR-файле, подпись которого проверяется, не существует файлов Digest.CP и Sign.CP, то файл не содержит подписей и никакой проверки не требуется;
- если такие файлы имеются, то в первую очередь осуществляется подсчет хэшей всех классов подписанного JAR-файла, не входящих в директорию META-INF, и проверка соответствия результата значениям хэшей, содержащихся в файле Digest.CP. Если результаты различны, то выдается Exception (считается, что JAR-файл поврежден);
- если хэши сошлись, то осуществляется собственно проверка подписи:
  - если задан конкретный сертификат (командой `-cert`), то производится поиск соответствующего сертификата в файле Sign.CP и, если такой сертификат найден, осуществляется проверка соответствующей подписи;
  - в противном случае осуществляется проверка всех подписей, содержащихся в файле Sign.CP. При этом после проверки на экран выводится информация о всех неверных подписях.

21.3. Контроль целостности JAR-файла провайдера

При загрузке провайдера «КриптоПро JCP» версия 2.0 осуществляется проверка подписей трех файлов `jcp.jar`, `ASN1P.jar` и `asn1rt.jar` на заданном ГОСТ сертификате (сертификат "прошит" в классе JarChecker), а также выполняется проверка DSA-подписи на SUN'овском сертификате.

Контроль целостности осуществляется при помощи функции check() класса JarChecker, которая запускается в классе Starter загружаемого провайдера, собранного с отключенным флагом DEBUG. Для корректной работы данной функции сертификат прошит в самом классе JarChecker, и указание пути к файлу с сертификатом при осуществлении контроля целостности не требуется.

22.Командная строка CPVerify

Командная строка CPVerify введена для более удобного контроля целостности а также возможности администрирования систем, в которых отсутствует графическое расширение или пакеты Java AWT и Swing.

С помощью командной строки можно создавать хранилища хэшей, добавлять в них файлы, удалять файлы из хранилища, пересчитывать и проверять хэши файлов в хранилище, а также работать с основным системным хранилищем.

22.1.Общий синтаксис вызова

Командной строке Prompt всегда передается следующий набор параметров:

```
doing repository [params]
```

Параметр **doing** определяет действие, требуемое от командной строки. Он обязательно должен стоять первым. Значения параметра приведены в таблице:

параметр	действие
-verify	Проверить файлы в хранилище. Команда проверяет хэши одного или нескольких файлов из указанного хранилища.
-make	Пересчитать хэши файлов в хранилище. По команде пересчитывается хэш одного или нескольких файлов в хранилище.
-add	Добавить файлы в хранилище. Команда добавляет один или несколько файлов в хранилище, и пересчитывает для них хэш.
-delete	Удалить файлы из хранилища. Команда удаляет один или несколько файлов из хранилища.
-create	Создать хранилище. Команда создает новое хранилище. Если хранилище уже существует, то оно будет перезаписано.
-check	Проверить статус хранилища. Команда проверяет статус хранилища: не повреждено или не удалено ли оно.
-setdefault	Сделать хранилище основным системным. Основное системное хранилище - то, в котором хранятся хэши наиболее важных системных файлов, и которое периодически проверяют внутренние службы криптопровайдера.
-getdefault	Узнать, какое хранилище является основным системным.
-print	Вывести состояние всех файлов в хранилище. Команда выводит состояние всех файлов в хранилище: не повреждены ли они, не удалены ли.
-help	Вывести справку. Общая справка по всем командам.

Параметр **repository** является необходимым во всех командах, кроме **-help** и **-getdefault**. Он задает хранилище, с которым будет проводиться операция. Он может быть определен одним из трех следующих способов:

параметр	хранилище
-repfile filename	Хранилище - файл, с именем filename
-reppref	Хранилище расположено в каталоге системных настроек (реестр для Windows).
-repdefault	Основное системное хранилище

Параметр **repository** может быть любым по счету, но не первым. Если он равен **-repfile**, следующее слово в командной строке считается именем файла.

Параметры [**params**] зависят от команды. Для всех команд действует параметр **-help** - подробная справка по команде. Команды **-help**, **-print**, **-getdefault**, **-setdefault**, **-check**, **-create** не предполагают дополнительных параметров. В командах **-verify**,

-make, **-add**, **-delete** надо определять список файлов, над которыми производится действие, специальными параметрами, указанными ниже в таблице:

Команда	**Параметр, определяющий файлы**	**Действие**
-verify	-all	Проверить все файлы, лежащие в хранилище.
	-file filename1 [-file filename2 [...]]	Проверить файлы filename1, filename2,..., если они есть в данном хранилище.
-make	-all	Пересчитать хэши всех файлов, лежащих в хранилище
	-file filename1 [-file filename2 [...]]	Пересчитать хэши файлов filename1, filename2,..., лежащих в хранилище
-add	-file filename1 [-file filename2 [...]]	Добавить в хранилище файлы filename1, filename2,...
-delete	-all	Удалить все файлы из хранилища
	-file filename1 [-file filename2 [...]]	Удалить файлы filename1, filename2,... из хранилища.

Любая команда из тех, которые изменяют хранилище, перед сохранением хранилища вызывает проверку всех файлов, в нем содержащихся. Поэтому если какие-то файлы в хранилище повреждены, его состояние можно перезаписать только удалив их всех из него одной командой **-delete**, или пересчитав для всех хэш.

Приложение завершается с ошибкой (выход по исключению), если возникла непредвиденная ситуация (отказано в доступе к файлу, ошибка ввода-вывода и т.д.), или если возникла ошибка при работе с хранилищем, когда оно считается существующим. Так, если проверяется статус поврежденного хранилища, приложение завершится нормально, выдав диагностическое сообщение, однако если проводится проверка файлов в поврежденном хранилище, приложение завершится с ошибкой. Приложение завершается нормально, если проверяемый файл из хранилища поврежден, выдавая соответствующую диагностику.

22.2.Список файлов, добавляемых в хранилище для контроля целостности.

Перед началом работы с провайдером необходимо создать основное хранилище в системных настройках, права на изменения которого даны только администратору. В него следует добавить исполняемые файлы Java, файлы содержащие пакеты java.lang, java.security, java.io, javax, системные библиотеки, конфигурационные файлы Java-машины, модули «КриптоПро JCP» версия 2.0, которые находятся в каталоге [путь к JRE]/lib/ext.

Этот список следует проверять средствами командной строки в отдельном процессе до загрузки рабочей Java-машины не реже одного раза в сутки.

В случае, если CPVerify зафиксирует изменение хотя бы одного элемента Java-машины, использование криптопровайдера следует прекратить до выяснения и устранения причин возникновения ошибки.

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

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

1. Использование шифровальных средств для криптографической защиты информации подлежит лицензированию в соответствии с действующим законодательством РФ.
2. Рабочие места, на которые установлены СКЗИ, должны быть аттестованы комиссией. Результаты работы комиссии отражаются в Акте готовности к работе
3. Правом доступа к рабочим местам с установленным СКЗИ должны обладать только лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, использующего СКЗИ, с правилами пользования или с другими нормативными документами, созданными на их основе.
4. Должностные инструкции администратора безопасности (его заместителя) и ответственного исполнителя должны учитывать требования настоящих Правил.
5. При каждом включении рабочей станции с установленным СКЗИ необходимо проверять сохранность печатей системного блока и разъемов рабочей станции.
6. Администратор безопасности должен периодически (не реже 1 раза в 2 месяца) проводить контроль целостности и легальности установленных копий ПО на всех АРМ со встроенной СКЗИ с помощью программ контроля целостности.
7. В случае обнаружения "посторонних" (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией в составе представителей служб информационной безопасности организации - владельца сети и организации - абонента сети, где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения.
8. Не допускается оставлять без контроля вычислительные средства, входящие в состав СКЗИ, при включенном питании и загруженном программном обеспечении СКЗИ. При кратковременном перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана производится с использованием пароля доступа.
9. Пользователь должен запускать только те приложения, которые разрешены администратором безопасности.
10. Средствами BIOS должна быть исключена возможность отключения пользователями ISA-устройств.
11. ПО, установленное на ПЭВМ, не должно иметь встроенных средств разработки и отладки программ.
12. ПЭВМ, обеспечивающие удаленный вход пользователей из глобальной сети, не должны использовать ПО СКЗИ.
13. Пароли, назначаемые пользователям, должны отвечать требованиям соответствующих инструкции и нормативных документов.

Не допускается:

1. Осуществлять несанкционированное копирование ключевых носителей.
2. Разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер (за исключением случаев, предусмотренных данными правилами).
3. Вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя.
4. Подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией.
5. Работать на компьютере, если во время его начальной загрузки не проходит встроенный тест ОЗУ, предусмотренный в ПЭВМ.
6. Вносить какие-либо изменения в программное обеспечение СКЗИ.
7. Изменять настройки, установленные программой установки СКЗИ или администратором.
8. Использовать синхропосылки, вырабатываемые не средствами СКЗИ.
9. Обрабатывать на ПЭВМ, оснащенной СКЗИ, информацию, содержащую государственную тайну.

10. Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ «КриптоПро JCP» версия 2.0.

11. Осуществлять несанкционированное вскрытие системных блоков ПЭВМ.

12. Приносить и использовать в помещении, где размещены средства СКЗИ, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер).

24.Литература

1. [РФ.Защита]. Закон РФ № 24-ФЗ от 20.02.95 г. "Об информации, информатизации и защите информации".
2. [РФ.ГосТайна]. Закон РФ № 5485-1 от 21.07.93 г. "О государственной тайне".
3. [РФ.Безопасность]. Закон РФ № 2446-1 от 05.03.92 г. "О безопасности".
4. [РФ.Связь]. Закон РФ № 15-ФЗ от 16.02.95 г. "О связи".
5. [РФ.Серификация]. Закон РФ № 5151-1 от 10.06.93 г. "О сертификации продукции и услуг".
6. [РФ.Стандартизация]. Закон РФ № 5154-1, 1993 г. "О стандартизации".
7. [РФ.Изменения]. Закон РФ № 4871-1, 1993 г. "Об обеспечении единства измерений".
8. [РФ.Органы связи]. Закон РФ № 4524-1 от 19.02.93 г. "О федеральных органах правительственной связи и информации".
9. [РФ.ГК]. Гражданский кодекс Российской Федерации. Ч. 1. Принят Государственной Думой 21 октября 1994 г. Одобрен Советом Федерации.
10. [ГОСТ 34003]. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
11. [ГОСТ 28147]. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
12. [ГОСТ 341001]. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
13. [ГОСТ 3411]. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.
14. [ГОСТ 50739]. ГОСТ Р 50739-95. Государственный стандарт Российской Федерации. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
15. [ГОСТ 1]. ГОСТ Р 1.0-92. Государственная система стандартизации Российской Федерации. Основные положения.
16. [ГОСТ 16487]. ГОСТ 16487-83. Делопроизводство и архивное дело. Термины и определения.
17. [ГОСТ 50922]. ГОСТ Р 50922-96. Государственный стандарт Российской Федерации. Защита информации. Основные термины и определения.
18. [Лицензирование]. Положение о государственном лицензировании деятельности в области защиты информации. Утверждено Решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации № 10 от 27 апреля 1994 г.
19. [ГТК Термины]. Гостехкомиссия России. Руководящий документ. Защита от НСД к информации. Термины и определения. - М.: Воениздат, 1992.
20. [ГТК защита]. Гостехкомиссия России. Концепция защиты информации в системах ее обработки, 1995.
21. [ГТК НСД]. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники (СВТ) и автоматизированных систем от НСД к информации. Москва, 1992 г.
22. [ГТК Классификация]. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. Москва, 1992 г.
23. [ГТК Показатели]. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. Москва, 1992 г.
24. [Халянин]. Халянин Д.В., Ярочкин В.И. Основы защиты промышленной и коммерческой информации. Термины и определения: Словарь / ИПКИР. - М., 1994.
25. [Бияшев]. Бияшев Р.Г., Диев С.И., Размахнин М.К. Основные направления развития и совершенствования криптографического закрытия информации / Зарубежная радиоэлектроника. 1989. № 12. С. 76-91.
26. [Словарь]. Толковый словарь по информатике. - М.: Финансы и статистика, 1991.
27. [Терминология]. Терминология в области защиты информации: Справочник / ВНИИстандарт, 1993.
28. [Формуляр]. ЖТЯИ.00091-01 30 01. КриптоПро JCP. Формуляр.
29. ЖТЯИ.00091-01 33 01. КриптоПро JCP. Руководство программиста.

30. ЖТЯИ.00091-01 90 01. КриптоПро JCP v. 2.0. Руководство администратора безопасности

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

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

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

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

35. [ПКЗ-2005]. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

36. Джим Яворски, Пол Дж. Перроун. "Система безопасности Java 2 Руководство разработчика." М. Издательский дом "Вильямс", 2001 ISBN 5-8459-0165-0 (рус)

25.Приложение 1. Акт готовности к работе

УТВЕРЖДАЮ

_____

(должность)

_____

(наименование учреждения)

_____

(подпись) (Ф.И.О.)

АКТ

готовности к работе _____ /наименование учреждения/ с _____ /наименование изделий/ "_____" _____ 20___г.

Комиссия в составе председателя _____ /должность/ _____ /Ф.И.О/ и членов назначенная _____ составила настоящий акт о том, что помещение эксплуатирующего органа _____ /название/, _____ /размещение/, хранилища ключевых носителей, охрана помещений и подготовленность сотрудников к обслуживанию _____/оборудование/ соответствуют: _____ /ГОСТ, инструкция, руководящие документы, правила пользования и т.п./

Комиссия отмечает, что инсталляция ПО вышеупомянутых изделий проведены в соответствии с _____ _____ инструкции

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

Председатель:	Члены комиссии
_____	_____
(подпись)	(Ф.И.О)
_____	_____
(подпись)	(Ф.И.О)
_____	_____
(подпись)	(Ф.И.О)
_____	_____
(подпись)	(Ф.И.О)

М.П.

26.Приложение 2. Журнал регистрации администраторов безопасности и пользователей

п/п	Организация	Ф.И.О. администратора безопасности пользователя системы	Данные регистрации	Дата регистрации	Дата выбытия	Примечание (пользователь, администратор)
	1	Сидоров А. А	нет	21.04.2000		Администратор безопасности
	2	Иванов И. И.	Почтовый адрес: a.sidorov@acme.ru Должность:	01.05.2000		Оператор расчетной системы

27.Приложение 3. Журнал пользователя сети

п/п	Дата	Время	Ф.И.О.пользователя системы	Событие	Дополнительные данные	Примечание
1	02.05.2000	09:00	Иванов И.И.	Поломка ключа		