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

Средство Криптографической Защиты Информации

КриптоПро CSP

Версия 2.0

Правила пользования

ЖТЯИ.00005-01 90 07

Листов 42

2002 г.

Содержание

1. Аннотация

Данный документ описывает основные правила пользования, связанные с установкой и эксплуатацией программно-аппаратных средств СКЗИ, рекомендации по размещению технических средств, использующих СКЗИ, рекомендации по проверке целостности установленного ПО, рекомендации по использованию средств криптографической защиты информации в различных автоматизированных системах и средствах вычислительной техники.

Дополнительно в разделе "Основные термины и положения" приводятся основные термины и определения, связанные с безопасностью и криптографической обработкой информации.

Данный документ может служить основой для разработки инструкций пользователям различных автоматизированных систем, использующих средства криптографической защиты информации.

2. Список сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
ITU-T	Международный комитет по телекоммуникациям (International Telecommunication Union)
IETF	Internet Engineering Task Force
ТМ	Устройство хранения информации на таблетке touch-memory
АС	Автоматизированная система
АРМ	Автоматизированное рабочее место
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
ЖМД	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 и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата открытого ключа абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей. Сетевой справочник.
ЦС	Центр Сертификации (Удостоверяющий Центр)

ЦР	Центр Регистрации
ФАПСИ	Федеральное агентство правительственной связи и информации при Президенте РФ
ЭД	Электронный документ
ЭЦП	Электронная цифровая подпись

3. Основные термины и положения

Автоматизированная информационная система

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

Автоматизированная система

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

Авторство информации

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

Актуальность информации

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

Администратор безопасности

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

Основные направления деятельности администратора безопасности:

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

Аутентификация

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

Аутентификация информации

Установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации, установление законным получателем (возможно арбитром) факта, что полученная информация наиболее вероятно была передана законным отправителем (источником) и что она при этом не заменена и не искажена. Любые преднамеренные и случайные попытки искажений информации обнаруживаются с соответствующей вероятностью [26].

Безопасность

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

Безопасность информации (информационная безопасность)

Состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п. [19].

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

Верификация

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

Владелец информации

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

Гриф конфиденциальности

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

Гриф секретности

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

Документ в электронной форме (Электронный документ)

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

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

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

Доступ к информации

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

Заверение (нотаризация)

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

Защита информации от НСД

Составная часть общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа. В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД, условно состоящей из следующих четырех подсистем: управления доступом; регистрации и учета; криптографической; обеспечения целостности [23].

Идентификация

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

Имитозащита

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

Имитовставка

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

Ключ (криптографический ключ)

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

Компрометация ключа

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

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

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

Конфиденциальность информации

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

Конфиденциальная информация

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

Криптографическая защита

Защита данных при помощи криптографического преобразования данных [11].

Криптографическое преобразование

Преобразование данных при помощи шифрования и (или) выработки имитовставки [11].

Нарушитель безопасности информации

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

Некорректный электронный документ

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

Несанкционированный доступ к информации (НСД)

1. Получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации [18]
2. Доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или автоматизированной системы (АС) [20] [22].

Носитель информации

Физическое лицо или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин [18].

Обработка информации

Передача, прием, хранение, преобразование и отображение информации.

Открытый ключ

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

Пароль

1. Идентификатор субъекта доступа, который является его (субъекта) секретом [20].
2. Секретная информация аутентификации, обычно представляющая собой строку знаков, которой должен обладать пользователь для доступа к защищенным данным.

Плановая смена ключей

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

Пользователь (потребитель) информации

1. Субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею [1].
2. Субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением [18].

Полномочный представитель организации

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

Проверка электронной подписи документа

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

Разглашение информации

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

Расшифрование данных

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

Сертификат открытого ключа

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

- имени субъекта или объекта системы, однозначно идентифицирующей его в системе;
- открытого ключа субъекта или объекта системы;
- дополнительных атрибутов, определяемых требованиями использования сертификата в системе;
- ЭЦП Издателя (Центра Сертификации), 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.

Секретный (закрытый) ключ

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

Система защиты информации

Совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации [18].

Система защиты информации от НСД

Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах [20].

Служебная и коммерческая тайна

1. Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами [9].
2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными Гражданским кодексом РФ и другими законами. Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору [9].

Средство криптографической защиты информации

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

Уничтожение информации

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

Управление ключами

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

Утечка информации

1. Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведкой [18].
2. Неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация доверена [25].

Функция хэширования

Заключается в сопоставлении произвольного набора данных в виде последовательности двоичных символов и его образа фиксированной небольшой длины, что позволяет использовать эту функцию в процедурах электронной цифровой подписи для сокращения времени подписи и проверки подписи. Эффект сокращения времени достигается за счет вычисления подписи только под образом подписываемого набора данных [12].

Целостность информации

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

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

Шифр

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

Шифрование

Процесс зашифрования или расшифрования [11].

Рисунок 1. Шифрование информации

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

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

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

Шифрование документов (текстов)

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

Электронная цифровая подпись

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

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

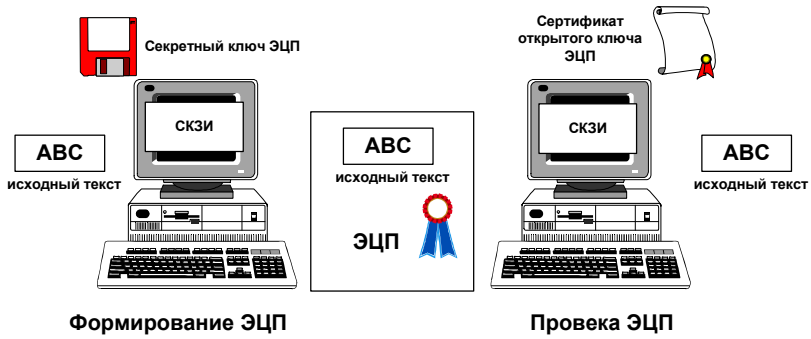

Рисунок 2. Формирование и проверка ЭЦП

Электронная цифровая подпись обеспечивает целостность сообщений (документов), передаваемых по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения, с гарантированной идентификацией ее автора (лица, подписавшего документ) [12].

Электронная цифровая подпись позволяет заменить при безбумажном документообороте традиционные печать и подпись. При построении цифровой подписи вместо обычной связи между печатью или рукописной подписью и листом бумаги выступает сложная математическая зависимость между электронным документом, закрытым и открытым ключами.

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

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

4. Основные технические данные и характеристики СКЗИ

СКЗИ КриптоПро CSP представляет средства защиты конфиденциальной информации, удовлетворяющие классу **КС1** в варианте исполнения 1; в варианте исполнения 2, отличающемся использованием сертифицированного средства защиты от НСД, и при условии обязательного опечатывания системного блока ПЭВМ - классу **КС2**.

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

4.1. Операционные системы

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

- Windows 98 с установленным ПО MS Internet Explorer версии 5.0 и выше;
- Windows 98 SE с установленным ПО MS Internet Explorer версии 5.0 и выше;
- Windows NT 4.0 SP5 и выше с установленным ПО MS Internet Explorer 5.0 и выше;
- Windows ME;
- Windows 2000;
- Windows XP.

На платформах Microsoft Windows 98/98SE/ME/NT/2000/XP, используемых с СКЗИ "КриптоПро CSP", должна быть произведена установка следующих двух пакетов обновлений:

1. Microsoft Security Bulletin MS02-048. Flaw in Certificate Enrollment Control Could

Allow Deletion of Digital Certificates (Q323172). August 28, 2002.
Доступ по адресу:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-048.asp

2. Microsoft Security Bulletin MS02-050. Certificate Validation Flaw Could Enable Identity Spoofing (Q328145). September 09, 2002.
Доступен по адресу:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-050.asp

Примечание. При выборе ОС необходимо учитывать следующие сроки поддержки и окончания эксплуатации операционных систем (по данным фирмы Microsoft на 03.07.2002 г.):

ОС	Поддержка	Окончание эксплуатации
Microsoft Windows 98	30 июня 2002 г.	30 июня 2003 г.
Microsoft Windows 98 SE	30 июня 2002 г.	30 июня 2003 г
Microsoft Windows NT 4/xx	30 июня 2002 г.	30 июня 2003 г
Microsoft Windows 2000	31 марта 2003 г.	
Microsoft Windows ME	31 Idекабря 2003 г.	

4.2. Реализуемые алгоритмы

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

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

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

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

4.3. Ключевые носители

Формирование закрытых ключей производится на следующие типы носителей:

- дискета 3,5";
- процессорные карты MPCOS-EMV, российские интеллектуальные карты (РИК), интеллектуальные карты "Оскар" с использованием считывателей смарт-карт, поддерживающий протокол pS/SC (GemPlus GCR-410, Towitoko, Oberthur OCR126);
- таблетки Touch-Memory DS1993 – DS1996 с использованием устройств Аккорд 4+, электронный замок "Соболь" или устройство чтения таблеток Touch-Memory DALLAS;
- электронный ключ с интерфейсом USB;
- сменный носитель с интерфейсом USB;
- реестр Windows (только для варианта исполнения 1).

Примечания. 1. Полный перечень устройств, поддерживающих различные носители ключевой информации, и требования по их использованию приведены в документе ЖТЯИ.00005-01 90 01 "КриптоПро CSP. Описание реализации".

2. Примечание. Допускается хранение закрытых ключей в реестре ОС Windows для варианта исполнения 2 при условии распространения на ПЭВМ требований по обращению с ключевыми носителями.

4.4. Длины ключей

Длина ключей электронной цифровой подписи

- закрытый ключ - 256 бит;
- открытый ключ - 1024 бита (ГОСТ Р 34.10-94)
  - 512 бит (ГОСТ Р 34.10-2001)

Длина ключей шифрования:

- сессионный ключ для шифрования по ГОСТ 28147-89 - 256 бит;
- закрытый ключ - 256 бит;
- открытый ключ - 1024 бита (на базе ГОСТ Р 34.10-94)
  - 512 бит (на базе ГОСТ Р 34.10-2001)

5. Ключевая система и ключевые носители

5.1. Общие положения

СКЗИ КриптоПро CSP является системой с открытым распределением ключей. Открытые ключи подписи и шифрования пользователей обычно представлены в виде сертификатов открытых ключей (см. "Основные термины и положения").

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

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

5.1.1. Шифрование данных

В СКЗИ КриптоПро CSP ключ зашифрования сообщения совпадает с ключом расшифрования (общий закрытый ключ связи), как описано в ГОСТ 28147-89. 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.

5.1.2. Формирование и проверка ЭЦП

Закрытый ключ подписи используется для выработки электронной цифровой подписи (см. "Основные термины и положения"). При проверке подписи проверяющий должен располагать открытым ключом (сертификатом) пользователя, поставившего подпись. Проверяющий должен быть полностью уверен в подлинности открытого ключа, а именно в том, что имеющийся у него открытый ключ соответствует открытому ключу конкретного пользователя. Для этой цели используется сертификат открытого ключа, подписанный третьей

доверенной стороной. Каждому пользователю, обладающему правом подписи, необходимо иметь:

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

5.2. Ключевой контейнер

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

Ключевой контейнер может содержать:

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

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

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

5.3. Структура ключевого контейнера

Ключевой контейнер содержит следующую информацию: главный ключ, маски главного ключа, имитовставка главного ключа, закрытые ключи, резервная копия главного ключа.

Примечание. Главным ключом считается один из закрытых ключей пользователя.

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

Структура ключевого контейнера обеспечивает чтение главного ключа и соответствующих ему масок отдельными операциями в раздельные области памяти, для чего он разбит на пять 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 (за исключением случаев, когда размер ключевого контейнера ограничен размерами памяти физического носителя).

5.4. Формирование ключей

Формирование ключей пользователя производится с использованием функции **CPGenKey** и спецификацией типа формируемого ключа: **AT_KEYEXCHANGE** или **AT_SIGNATURE**.

Формирование ключей возможно если:

- контекст криптопровайдера КриптоПро CSP открыт функцией **CPAcquireContext** с флагом **CRYPT_NEWKEYSET** и несуществующим именем ключевого контейнера, специфицированным параметром **pszContainer**;
- контекст криптопровайдера КриптоПро CSP открыт функцией **CPAcquireContext** с указанием ранее созданного ключевого контейнера, специфицированного параметром **pszContainer**.

Примечание.
1. При использовании считывателей смарт-карт или устройств чтения таблеток Touch-Memory DALLAS необходимо проверить настройки COM портов ПЭВМ в BIOS и ОС Windows. При

отключенных COM портах (**disabled**) работа со считывателями будет невозможна.

2. Перед использованием процессорных карт все карты должны быть выпущены. Для этого требуется наличие транспортного пин-кода и ПО выпуска карт, поставляемого дистрибутором..

3. При использовании НГМД в качестве ключевого носителя ключевой носитель, как любой гибкий диск, может быть поврежден. Во избежание потери ключевой информации рекомендуется хранить рабочую копию ключевой дискеты.

5.5. Хранение ключевых носителей

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

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

При хранении ключей в реестре Windows требования по хранению личных ключевых носителей распространяются на ПЭВМ (в том числе, после удаления ключей из реестра). Настоятельно рекомендуется использовать парольную защиту при хранении ключей в реестре ПЭВМ.

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

- в памяти приложения.
- в "Службе хранения ключей", которая реализована в виде системного сервиса Windows.

Примечание. Функционирование СКЗИ КриптоПро CSP в режиме "Службы хранения ключей" обеспечивает дополнительную защиту ключевой информации от других приложений, выполняющихся на ПЭВМ, но может незначительно снизить производительность. Настройка функционирования СКЗИ КриптоПро CSP производится согласно описанию, приведенному в разделе 10.5.

5.6. Сроки действия ключей

При использовании СКЗИ КриптоПро CSP на рабочих местах пользователей должны использоваться следующие сроки действия ключей:

- срок действия закрытого ключа – до 1 года 3 месяцев;
- срок действия открытого ключа (сертификата открытого ключа) 1024 бита – не больше 6 лет.

5.7. Уничтожение ключей на ключевых носителях

Ключи на ключевых носителях (включая Touch Memory и смарт-карты), срок действия которых истек, уничтожаются путем переформатирования (очистки) с использованием ПО СКЗИ КриптоПро CSP. Ключевые носители могут быть использованы в дальнейшем пользователями при условии записи на них новой ключевой информации.

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

6. Управление ключевой системой

Управление ключевой системой в АС базируется на сочетании организационных и программно-технических механизмов управления.

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

- центр управления ключевой системой (ЦУКС), включающий в себя администратора Центра Сертификации и администратора Центра Регистрации;
- администратор безопасности организации;
- пользователь.

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

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

- имя субъекта или объекта системы, однозначно идентифицирующее его в системе;
- открытый ключ субъекта или объекта системы;
- дополнительные атрибуты, определяемые требованиями использования сертификата в системе;
- ЭЦП Издателя (Центра Сертификации), заверяющую совокупность этих данных.

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

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

6.1. Центр управления ключевой системой

Центр управления ключевой системой является структурным подразделением, обеспечивающим выполнение следующих функций:

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

- получение и обработка сообщений о компрометации ключей пользователями;
- организация схемы оперативного оповещения пользователей обо всех изменениях, происходящих в сети (компрометация ключей, восстановление конфидециальной связи после компрометации ключей, включение новых пользователей, плановая смена ключей и т. п.);
- плановое изготовление списка отозванных сертификатов;
- разработка и поддержка функционирования парольной системы оповещения в сети;
- управление ключевой системой;
- разбор конфликтных ситуаций и доказательство авторства электронного документа, снабженного электронной цифровой подписью.

6.2. Формирование ключей пользователя

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

- регистрация пользователя;
- формирование пользователем личных ключей (запроса на сертификат);
- передача запроса в Центр Регистрации;
- верификация запроса Центром Регистрации;
- формирование сертификата пользователя;
- получение сертификата пользователем.

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

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

Формирование ключей пользователя происходит в следующей последовательности.

6.2.1.Регистрация пользователя

1) Пользователь системы или администратор безопасности лично представляют в Удостоверяющий Центр (Центр Регистрации) документы, необходимые 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 выводятся на принтер в двух экземплярах и заверяются 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 ЦУКС и пользователя (см. Рисунок 3. Карточка оповещения о компрометации).

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

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

каналам общего пользования. **Карточка оповещения** должна храниться у пользователя наравне с ключами.

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

Рисунок 3. Карточка оповещения о компрометации

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

6) Администратор ЦР делает запись в "Журнале регистрации администраторов безопасности и пользователей".

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

6.2.2.Ключ и сертификат пользователя

При формировании закрытого ключа и сертификата используются следующие значения.

Длина открытого ключа – 1024 бита.

Сроки действия:

- срок действия закрытого ключа пользователя– до 1 года 3 месяцев;
- срок действия сертификата пользователя (1024 бита) – до 6 лет.
-

6.2.3.Формирование личных ключей пользователя

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

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

2) Пользователь производит формирование личного закрытого ключа и запроса на сертификат, содержащий открытый ключ пользователя.

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

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

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

6) Если запрос был записан на магнитный носитель, пользователь (администратор безопасности) прибывают в Центр Регистрации (ЦУКС) 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 Регистрации, используя для этого доступные способы доставки (например, заказное письмо).

8) При получении запроса на сертификат администратор (ЦС) ЦР 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".

6.2.4.Получение личного сертификата пользователем

Личный сертификат может быть получен следующими способами:

- при личном присутствии пользователя (администратора безопасности) в ЦУКС;
- 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).

6.3. Повторная регистрация пользователя

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

6.4. Плановая смена ключей

6.4.1.Смена ключей пользователя

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

Формирование нового закрытого ключа, запроса на сертификат, передача запроса в ЦР и получение сертификата производится согласно последовательности, описанной в разделе 6.2 "Формирование ключей ".

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

6.5. 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 ключи после проведения служебного расследования уничтожаются (см. раздел "Уничтожение ключей на ключевых носителях"), о чем делается запись в "Журнале пользователя сети".

6.5.1.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 (ЦУКС) о компрометации ключей пользователя.

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

оповещения о компрометации" (см. Рисунок 3. Карточка оповещения о компрометации).

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

6.5.2.Действия ЦУКС при компрометации ключей пользователя

При получении сообщения о компрометации ключа одного из пользователей сети, администратор ЦР оповещает ЦС о необходимости добавления в список отозванных сертификатов сертификата, соответствующего скомпрометированному закрытому ключу. 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. 6.2.1 "Регистрация пользователя"), может быть использована электронная почта.

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

6.6. Исключение пользователя из сети

Исключение пользователя из сети может быть осуществлено на основании письменного заявления пользователя в адрес начальника ЦУКС, заверенного руководством организации. Исключение пользователя из сети аналогично производится аналогично действиям компрометации ключа пользователя. Получив такое заявление, администратор ЦР производит действия, описанные в разделе 6.5.2 "Действия ЦУКС при компрометации ключей пользователя".

6.7. Ведение журналов

Администратор ЦУКС ведет следующие журналы:

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

Администраторы безопасности организации ведут журнал "Журнал пользователя сети".

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

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

В "Журнале пользователя сети" может отражаться следующая информация:

- дата, время;
- запись о компрометации ключа;
- запись об изготовлении личного ключевого носителя пользователя, идентификатор носителя;
- запись об изготовлении копий личного ключевого носителя пользователя, идентификатор носителя;

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

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

7. Модуль поддержки сетевой аутентификации

При использовании в составе СКЗИ модуля поддержки сетевой аутентификации ЖТЯИ.00101-01 99 01 необходимо руководствоваться документом: КриптоПро CSP. Руководство по использованию модуля поддержки сетевой аутентификации КриптоПро TLS. ЖТЯИ.00101-02 90 01.

8. Нештатные ситуации при эксплуатации СКЗИ

Ниже (Таблица 8-1) приведен основной перечень нештатных ситуаций и соответствующие действия персонала при их возникновении.

Таблица 8-1. Действия персонала в нештатных ситуациях

№ п/п	Нештатная ситуация	Действия персонала
1.	Компрометация одного из личных ключевых носителей.	Порядок действий при компрометации ключей описан в разделе 6.5.1 "Компрометация ключей пользователя".
2.	Выход из строя первого личного ключевого носителя. Аналогично для носителей Touch Memory и смарт-карт.	Необходимо сообщить по телефону в ЦУКС о факте выхода из строя личного ключевого носителя и обеспечить его доставку в ЦУКС для выяснения причин выхода из строя. Для работы используется второй личный ключевой носитель..
3.	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 ЦУКС для повторной регистрации (без изменения данных регистрации).
4.	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.
5.	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.
6.	Утеря личного ключевого носителя.	Утеря личного ключевого носителя приводит к компрометации ключей. Порядок действий при компрометации ключей описан в разделе 6.5.1 "Компрометация ключей пользователя".

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

Все нештатные ситуации должны отражаться в соответствующем журнале: "Журнал пользователя сети" (см. 6.7 "Ведение журналов").

9. Рекомендации по размещению технических средств с СКЗИ

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

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

8. Перед вскрытием помещений должна быть проверена целостность оттисков печатей и исправность замков. При обнаружении нарушения целостности оттисков печатей, повреждения замков или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, помещение не вскрывается, а о случившемся немедленно ставится в известность руководство и отдел безопасности.
9. В случае утраты ключа от входной двери помещения немедленно ставится в известность отдел безопасности учреждения.
10. На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководством учреждения, в которых предусматривается порядок вызова администрации, должностных лиц, вскрытие помещений, очередность и порядок спасения конфиденциальных документов и дальнейшего их хранения.
11. Рекомендуется не использовать в помещении, где размещены рабочие места с установленным СКЗИ, радиотелефоны и другую радиоаппаратуру.

10. Установка ПО СКЗИ на ПЭВМ

10.1. Требования к системе

ПО СКЗИ КриптоПро CSP предназначено для использования в операционных системах Windows 95/98/ME/NT/2000/XP на ПЭВМ типа IBM PC с процессором Pentium и выше.

Примечание. Перечень операционных систем и дополнительные требования, необходимые для функционирования СКЗИ КриптоПро CSP, приведены в документе ЖТЯИ.00005-01 90 01 "КриптоПро CSP. Описание реализации".

В состав дополнительных аппаратных средств ПЭВМ может входить средство для обеспечения контроля целостности ПО и предотвращения загрузки ОС с нештатных носителей.

10.2. Контроль целостности дистрибутива

Программа **CPVERIFY.EXE** поставляется вместе с дистрибутивом и предназначена для контроля целостности дистрибутивов, изготовленных организацией-разработчиком ПО.

Примечание. Программа CPVERIFY.EXE является средством проверки целостности дистрибутива и не заменяет собой средства контроля целостности уже установленного ПО.

Синтаксис командной строки для запуска программы **CPVERIFY.EXE** выглядит следующим образом:

- Проверка целостности заданного файла с использованием значения хеш-функции.

```
cpverify.exe filename hashvalue

   filename  - имя проверяемого файла.

   hashvalue - ранее вычисленное значение хеш-функции, 64 символа.
```

При проверке целостности дистрибутивного файла, значение хэш-функции вводится из лицензионного бланка.

В случае успешного завершения проверки программа выдает сообщение **"File ‘filename’ has been verified"**, где ‘filename’ – имя проверяемого файла и возвращает ненулевой код возврата.

Нулевой код возврата и вывод сообщения на экран **"File ‘filename’ was corrupted"** обозначает несоответствие значения хеш-функции, вычисленной разработчиком для дистрибутива, и свидетельствует об изменениях исходного файла. В данном случае процесс установки дистрибутива ПО СКЗИ КриптоПро CSP должен быть прерван.

10.3. Установка дистрибутива ПО СКЗИ КриптоПро CSP

Установка дистрибутива должна производится пользователем, имеющим права администратора.

Перед установкой дистрибутива ПО СКЗИ КриптоПро CSP, удалите все ранее существующие версии устанавливаемого ПО. Для этого используете пункты основного меню Windows "**Пуск**", "**Настройка**", "**Панель управления**", "**Установка и удаление программ**" (см. Рисунок 4).

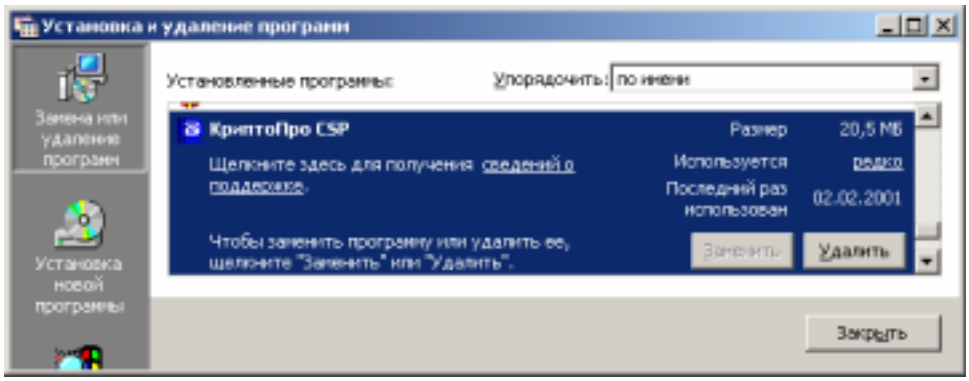

Рисунок 4. Удаление предыдущей версии ПО

Установка программного обеспечения производится путем запуска программы **CPCSP.EXE (**или программы **SETUP.EXE**, находящейся на первом диске дистрибутива, если дистрибутив записан на несколько магнитных носителей - дискет). Для запуска программы используете пункты "**Пуск**", "**Выполнить**" главного окна Windows.

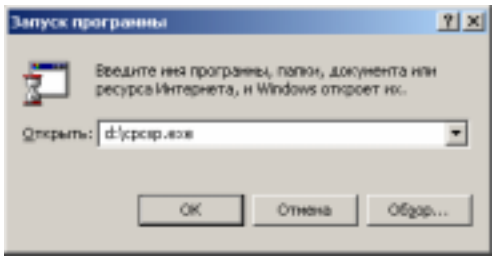

Рисунок 5. Запуск ПО установки

При установке дистрибутива дальнейшая установка производится в соответствии с сообщениями, выдаваемыми ПО установки.

После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

10.4. Изменение набора устройств хранения ключевой информации

Программа установки по умолчанию устанавливает все модули, обеспечивающие работу с различными поддерживаемыми устройствами хранения ключевой информации, но при этом настойки СКЗИ КриптоПро CSP допускают использовать в качестве ключевого носителя только дискету 3,5". Если для работы с ПО СКЗИ необходимы дополнительные типы устройств работы с ключевыми носителями, выберите режим изменения их состава.

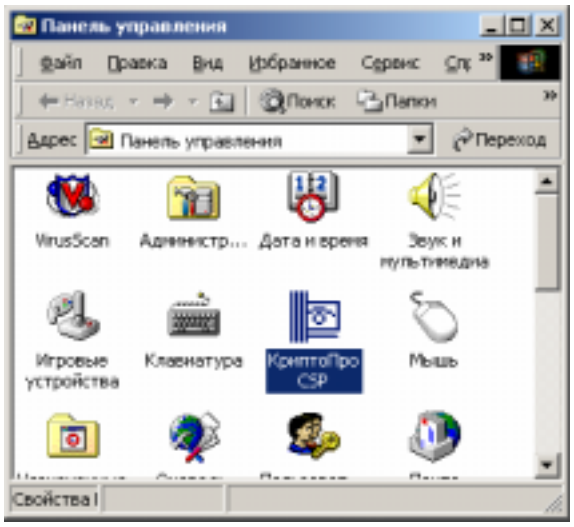

Рисунок 6. Панель управления

Для этого откройте панель управления компьютером, используя пункты меню "**Пуск**", "**Настройка**", "**Панель управления**" и в окне панели управления (см. Рисунок 6) выберите значок "**КриптоПро CSP**". В панели настройки СКЗИ КриптоПро CSP (см. Рисунок 7) выберите закладку "**Оборудование**" и, нажав кнопку "**Настроить считыватели**", добавьте (или удалите) из списка те устройства, которые будут использованы в качестве считывателей ключевой информации (см. Рисунок 8).

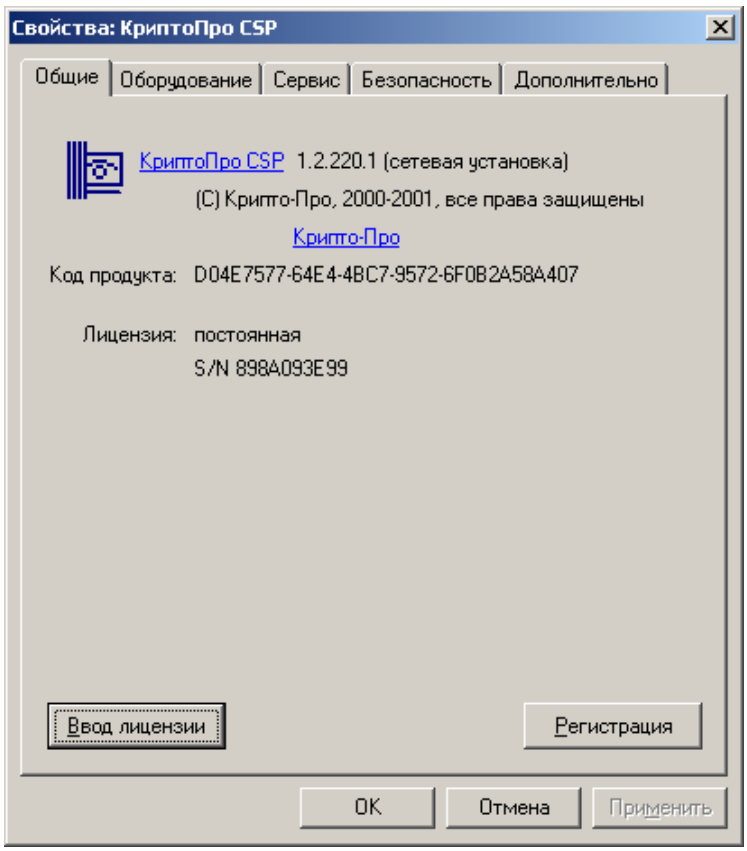

Рисунок 7. Панель настройки

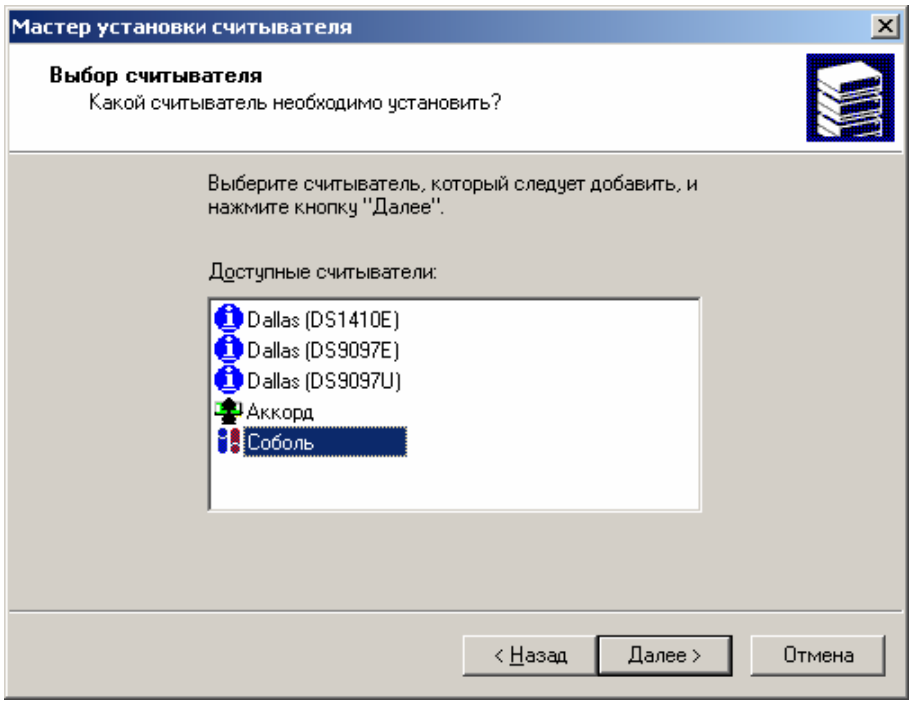

Рисунок 8. Добавление устройства хранения ключей

Примечание. В состав дистрибутива СКЗИ КриптоПро CSP не входят драйвера и другие модули третьих производителей, обеспечивающие взаимодействие СКЗИ с аппаратной частью. Для их установки нужно воспользоваться программой установки, поставляемой производителями таких устройств, либо получить их с сервера разработчика СКЗИ КриптоПро CSP по адресу http://www.cryptopro.ru / CryptoPro / moduls.html. Например, если CSP уже установлен и нужно использовать новые устройства, необходимо установить поддерживающие драйвера и другие модули от производителей этих устройств.

Программное обеспечение СКЗИ КриптоПро CSP распространяется с ограниченным использованием по времени – 30 дней (см.). До истечения этого срока пользователь должен ввести серийный номер и код активации с Лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (Дилера).

В панели настройки СКЗИ КриптоПро CSP (см. Рисунок 7) выберите пункт "**Ввод лицензии**" и введите **серийный номер** и **ключ активации** с бланка **Лицензии** (см. Рисунок 9).

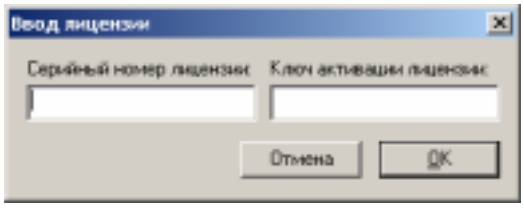

Рисунок 9. Ввод данных лицензии

После завершения программы установки рекомендуется зарегистрировать установленное ПО СКЗИ КриптоПро CSP у организации-разработчика. Для этого откройте панель управления компьютером, используя пункты меню "**Пуск**", "**Настройка**", "**Панель управления**" и в окне панели управления (см. Рисунок 6) выберите значок "**КриптоПро CSP**".

В панели настройки СКЗИ КриптоПро CSP (см. Рисунок 7) выберите пункт **Регистрация**, и выполните регистрацию.

10.5. Настройка ПО СКЗИ

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

- В памяти приложения.
- В "Службе хранения ключей", которая реализована в виде системного сервиса.

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

Для изменения режима функционирования СКЗИ откройте панель настроек СКЗИ КриптоПро CSP как описано в предыдущем пункте и выберите необходимый режим (см. Рисунок 10).

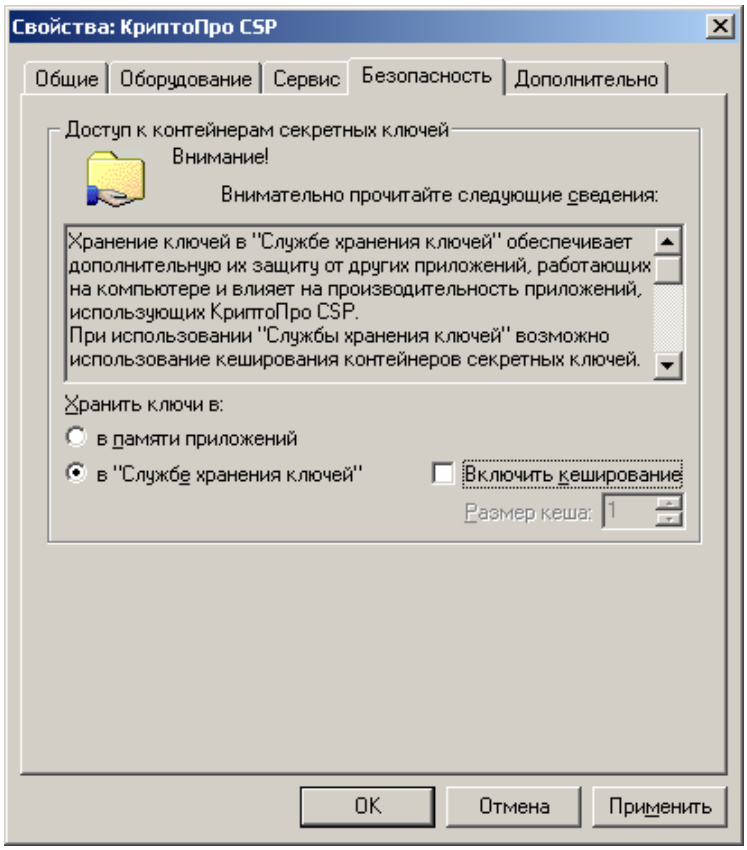

Рисунок 10. Настройка режима работы СКЗИ

10.6. Использование ключей и сертификатов на другом компьютере

Реализация КриптоПро CSP позволяет хранить личные сертификаты пользователя не только в локальном справочнике сертификатов компьютера, а так же вместе с личными ключами пользователя на ключевом носителе (при условии, что ключевой носитель имеет достаточный объем памяти для записи сертификата). Хранение сертификата на ключевом носителе позволяет пользователю переносить всю необходимую ключевую информацию с компьютера, где был сформирован ключ пользователя на другие рабочие места.

Для того, чтобы воспользоваться личными ключами и сертификатами пользователя в различных приложениях на другом компьютере, необходимо на этом компьютере установить пользовательский сертификат в локальный справочник и создать ссылку, которая будет однозначно связывать сертификат с личным ключом пользователя.

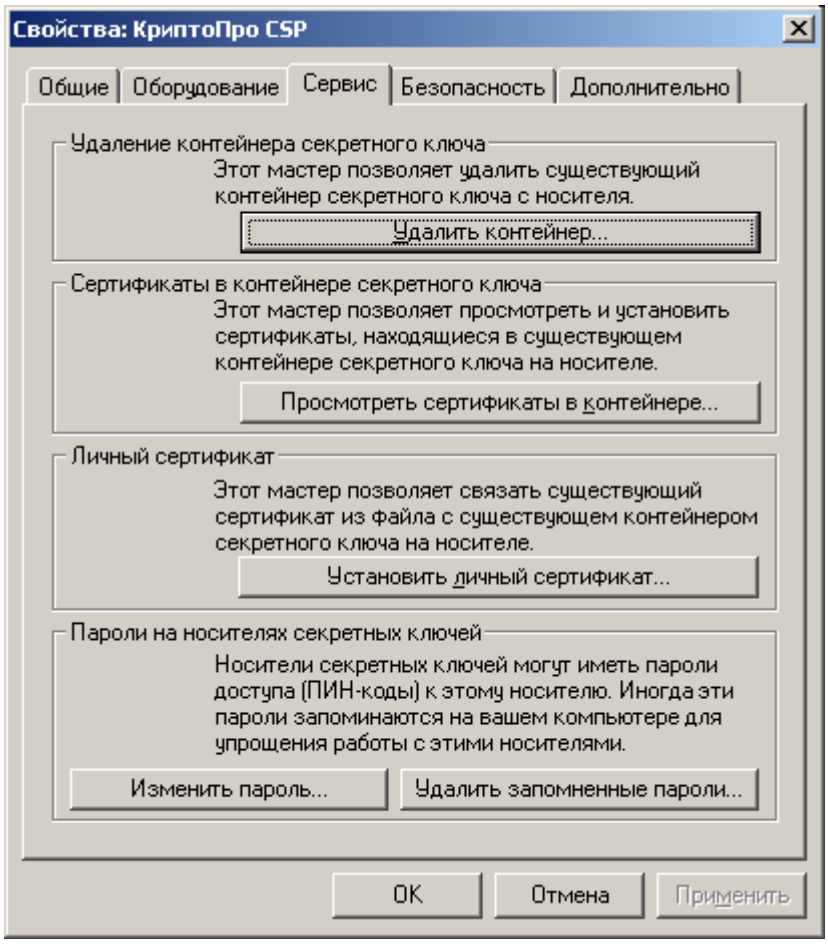

Рисунок 11. Установка сертификата

Для этого, используя пункты меню **Пуск, Настройка, Панель управления** в окне панели управления выберите значок **КриптоПро CSP**. В отображаемом окне диалога выберите закладку **Оборудование** и нажмите кнопку **Сертификаты в контейнере секретного ключа** (см. Рисунок 11).

Ключевой носитель, содержащий личный ключ и сертификат, при этом должен быть вставлен в соответствующее устройство считывания.

Если на ключевом носителе содержится сертификат, его содержание будет отображено в стандартном окне просмотра сертификатов. Нажмите кнопку **Установить сертификат** для его переноса с ключевого носителя в локальный справочник (см. Рисунок 12).

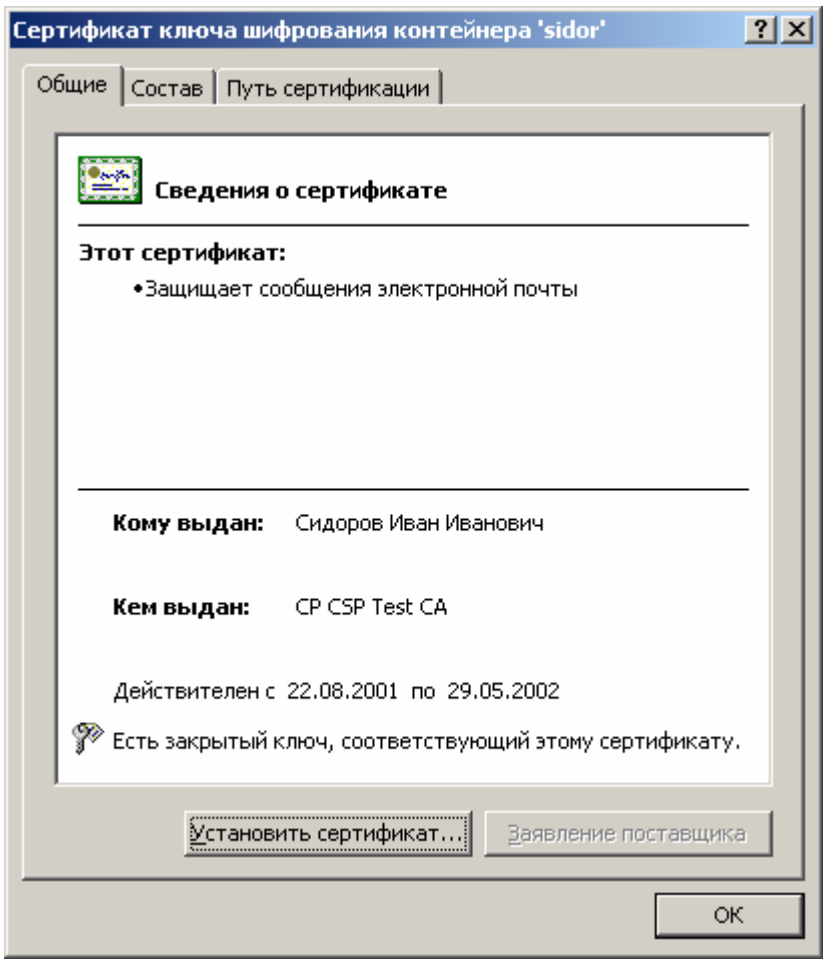

Рисунок 12. Отображение сертификата

10.7. Рекомендации по установке ПО СКЗИ

После завершения процесса установки ПО СКЗИ должны быть выполнены действия, необходимые для осуществления регулярного контроля установленного СКЗИ с помощью ПО контроля целостности и/или ПАК "Аккорд-АМДЗ", электронного замка "Соболь".

При установке программного обеспечения КриптоПро CSP, следует руководствоваться следующими рекомендациями:

1. Аппаратуру, на которой устанавливается СКЗИ, рекомендуется проверить на отсутствие аппаратных закладок.
2. Все программное обеспечение ПЭВМ, на которой будет устанавливаться СКЗИ, должно быть лицензионно чистым, при этом рекомендуется не допускать наличия средств разработки и отладки программ.
3. Перед установкой СКЗИ необходимо проверить программное обеспечение ПЭВМ на отсутствие вирусов и программных закладок.
4. Для обеспечения защиты от НСД могут использоваться: ПАК "Аккорд-АМДЗ", электронный замок "Соболь".
5. Дополнительно могут быть предприняты меры, препятствующие извлечению платы защиты от НСД из ПЭВМ - системные блоки ПЭВМ могут быть опечатаны специально выделенной для этих целей печатью. Наряду с этим допускается применение других средств контроля доступа к ПЭВМ.
6. К эксплуатации программного обеспечения, имеющего в своем составе СКЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие эксплуатационную документацию на соответствующие программные средства.
7. После завершения процесса установки должны быть выполнены действия, необходимые для осуществления ежедневного контроля установленного ПО, а также его окружения.

11. Требования по защите от НСД ПО СКЗИ

Средства СКЗИ КриптоПро CSP обеспечивают защиту конфиденциальной информации по уровню КС1 для варианта исполнения 1 и по уровню КС2 - для варианта исполнения 2 СКЗИ.

11.1. Принципы защиты информации от НСД

Защита информации от НСД 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;
- наличие администратора службы 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.

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

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

11.2. Организационные меры защиты от НСД

При использовании СКЗИ «КриптоПро CSP» должны соблюдаться следующие организационные меры:

1. Право доступа к рабочим местам с установленным ПО СКЗИ «КриптоПро CSP» предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе СКЗИ «КриптоПро CSP».

2. Запрещается осуществление несанкционированного администратором безопасности копирование ключевых носителей.

3. Запрещается разглашение содержимого ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер.

4. Запрещается использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ «КриптоПро CSP», либо использовать ключевые носители на посторонних ПЭВМ.

5. Запрещается запись на ключевые носители посторонней информации.

6. На технических средствах, оснащенных СКЗИ «КриптоПро CSP», должно использоваться только лицензионное программное обеспечение фирм-производителей.

7. На ПЭВМ, оснащенных СКЗИ «КриптоПро CSP», не допускается установка средств разработки и отладки ПО. Если средства отладки приложений необходимы для технологических потребностей пользователя, то их использование должно быть санкционировано администратором безопасности. В любом случае запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений,

использующих СКЗИ «КриптоПро CSP». Необходимо исключить попадание в систему программ, позволяющих, пользуясь ошибками ОС, получать привилегии администратора.

8. Должен быть исключен несанкционированный доступ посторонних лиц в помещения, в которых установлены технические средства СКЗИ «КриптоПро CSP», по роду своей деятельности не являющихся персоналом, допущенным к работе в указанных помещениях.

9. Запрещается оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ «КриптоПро CSP» после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

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

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

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

13. В BIOS ПЭВМ определяются установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске, должны быть: отключена загрузка с гибкого диска, привода CD-ROM, исключены прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Применение ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС, не допускается.

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

15. Вход в BIOS ПЭВМ должен быть защищен паролем. Пароль для входа в BIOS должен быть известен только администратору.

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

17. При загрузке ОС должен производиться контроль целостности программного обеспечения, входящего в состав СКЗИ «КриптоПро CSP», самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ.

18. Должно производиться физическое затирание содержимого удаляемых файлов.

19. Должны быть реализованы организационно-технические меры защиты от НСД в соответствии с разделом 15.3 Правил пользования администратора безопасности ЖТЯИ.00005-01 90 06.

20. Должны быть внесены изменения в системном реестре ОС Windows NT/2000/XP в соответствии с разделом 15.4 Правил пользования администратора безопасности ЖТЯИ.00005-01 90 06.

21. Должны быть дополнительные настройки ОС Windows 95/98 в соответствии с разделом 15.5 Правил пользования администратора безопасности ЖТЯИ.00005-01 90 06.

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

11.3.1. Программно-аппаратный комплекс "Аккорд-АМДЗ"

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

ПАК "Аккорд-АМДЗ" обеспечивает:

- идентификацию, проверку подлинности, разграничение доступа к ресурсам ПЭВМ на уровне выполняемых задач и контроль доступа субъектов в систему (ПЭВМ);

- регистрацию и учет входа (выхода) пользователей в систему (из системы), запуска (завершения) программ и процессов, доступа пользователей к защищаемым файлам, изменения полномочий пользователей;
- обеспечение целостности программных средств.

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

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

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

Установка программного обеспечения и аппаратной части комплекса "Аккорд-АМДЗ" на АРМ может выполняться специалистами поставщика СКЗИ или представителями службы информационной безопасности. Настройка комплекса "Аккорд-АМДЗ" на требуемую конфигурацию выполняется администратором безопасности. Настройка должна исключать возможность вмешательства пользователя в процессы загрузки операционной системы и прикладного ПО и проверки целостности программной среды.

11.3.2. Электронный замок "Соболь"

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

Система *Электронный замок* обеспечивает:

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

Установка и настройка электронного замка на АРМ пользователя должна производиться в соответствии с эксплуатационной документацией. Перед эксплуатацией электронного замка в составе АРМ пользователя необходимо ознакомиться с комплектом документации (в соответствии с паспортом УВАЛ.00300-04 ПС) на данный комплекс и принять рекомендуемые в документации защитные организационные меры.

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

12. Обеспечение безопасности функционирования рабочих мест со встроенной СКЗИ

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

Примечание. Использование шифровальных средств для криптографической защиты информации подлежит лицензированию в соответствии с действующим законодательством РФ.

1. Рабочие места, на которые установлены СКЗИ, должны быть аттестованы комиссией. Результаты работы комиссии отражаются в "Акте готовности к работе" (см. Приложение 1).
2. Правом доступа к рабочим местам с установленным СКЗИ должны обладать только лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, использующего СКЗИ, с настоящими Правилами пользования или с другими нормативными документами, созданными на их основе.
3. Должностные инструкции администратора безопасности (его заместителя) и ответственного исполнителя должны учитывать требования настоящих Правил.
4. Системные блоки ПЭВМ с установленным СКЗИ должны быть опечатаны специально выделенной для этих целей печатью. Наряду с этим допускается применение других дополнительных средств контроля за доступом к ПЭВМ.
5. Администратор безопасности должен периодически (не реже одного раза в два месяца) проводить контроль целостности и легальности установленных копий ПО на всех АРМ со встроенной СКЗИ с помощью программ контроля целостности.
6. 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.
7. 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.
8. При каждом включении рабочей станции с установленным СКЗИ необходимо проверять сохранность печатей системного блока и разъемов рабочей станции.
9. Пользователь должен запускать только те приложения, которые разрешены администратором безопасности.
10. На ПЭВМ должна быть установлена только одна ОС.
11. При использовании ПАК "Аккорд-АМДЗ" или электронного замка "Соболь" с интерфейсом ISA рекомендуется не использовать ПЭВМ с реализованной в BIOS функцией отключения использования ISA-устройств.
12. ПО, установленное на ПЭВМ, не должно иметь встроенных средств разработки и отладки программ.
13. Должны быть приняты меры по исключению вхождения пользователей в режим конфигурирования BIOS (например, с использованием парольной защиты).
14. Должна быть исключена возможность работы на ПЭВМ, если во время начальной загрузки не проходят встроенные тесты.
15. ПЭВМ, обеспечивающие удаленный вход пользователей из глобальной сети, (например RAS сервер) не должны использовать ПО СКЗИ.

16. Пароли, назначаемые пользователям, должны отвечать требованиям соответствующих инструкции и нормативных документов (ГТК, ЦБ РФ).
17. 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 (администраторами безопасности).

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 в комплектации.
5. Работать на компьютере, если во время его начальной загрузки не проходит встроенный тест ОЗУ, предусмотренный в ПЭВМ.
6. Вносить какие-либо изменения в программное обеспечение СКЗИ.
7. Изменять настройки, установленные программой установки СКЗИ или администратором.
8. Использовать синхропосылки, вырабатываемые не средствами СКЗИ.
9. Обрабатывать на ПЭВМ, оснащенной СКЗИ, информацию, содержащую государственную тайну.
10. Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ КриптоПро CSP.
11. Осуществлять несанкционированное вскрытие системных блоков ПЭВМ.
12. Приносить и использовать в помещении, где размещены средства СКЗИ, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер).

Литература

1. Закон РФ № 24-ФЗ от 20.02.95 г. "Об информации, информатизации и защите информации".
2. Закон РФ № 5485-1 от 21.07.93 г. "О государственной тайне".
3. Закон РФ № 2446-1 от 05.03.92 г. "О безопасности".
4. Закон РФ № 15-ФЗ от 16.02.95 г. "О связи".
5. Закон РФ № 5151-1 от 10.06.93 г. "О сертификации продукции и услуг".
6. Закон РФ № 5154-1, 1993 г. "О стандартизации".
7. Закон РФ № 4871-1, 1993 г. "Об обеспечении единства измерений".
8. Закон РФ № 4524-1 от 19.02.93 г. "О федеральных органах правительственной связи и информации".
9. Гражданский кодекс Российской Федерации. Ч. 1. Принят Государственной Думой 21 октября 1994 г. Одобрен Советом Федерации.
10. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
11. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

12. ГОСТ Р 34.10-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма.

13. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной подписи.

14. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.

15. ГОСТ Р 50739-95. Государственный стандарт Российской Федерации. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

16. ГОСТ Р 1.0-92. Государственная система стандартизации Российской Федерации. Основные положения.

17. ГОСТ 16487-83. Делопроизводство и архивное дело. Термины и определения.

18. ГОСТ Р 50922-96. Государственный стандарт Российской Федерации. Защита информации. Основные термины и определения.

19. Положение о государственном лицензировании деятельности в области защиты информации. Утверждено Решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации № 10 от 27 апреля 1994 г.

20. Гостехкомиссия России. Руководящий документ. Защита от НСД к информации. Термины и определения. - М.: Воениздат, 1992.

21. Гостехкомиссия России. Концепция защиты информации в системах ее обработки, 1995.

22. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники (СВТ) и автоматизированных систем от НСД к информации. Москва, 1992 г.

23. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. Москва, 1992 г.

24. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. Москва, 1992 г.

25. Халянин Д.В., Ярочкин В.И. Основы защиты промышленной и коммерческой информации. Термины и определения: Словарь / ИПКИР. - М., 1994.

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

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

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

29. ЖТЯИ.00005-01 30 01. КриптоПро CSP. Формуляр.

30. ЖТЯИ.00005-01 90 01. КриптоПро CSP. Описание реализации.

31. ЖТЯИ.00005-01 90 06. КриптоПро CSP. Правила пользования администратора безопасности.

32. ЖТЯИ.00101-02 90 01. КриптоПро CSP. Руководство по использованию модуля поддержки сетевой аутентификации КриптоПро TLS.

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.

Приложение 1. Акт готовности к работе

УТВЕРЖДАЮ

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

АКТ

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

"_____" _____ 199___г.

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

назначенная _____ составила настоящий акт о том, что помещение

эксплуатирующего органа _____, размещение _____, хранилища
название оборудование

ключевых документов, охрана помещений и подготовленность сотрудников к обслуживанию

_____
___ оборудование

соответствуют:

_____
__ (ГОСТ, инструкция, руководящие документы, правила пользования и т.п.)

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

_____
_____ инструкции

Вывод: комиссия считает, объект_____ отвечает требованиям
название объекта

_____
_____ название инструкции

по обеспечению безопасности связи по уровню _____ и может быть введен в действие.

Председатель:

_____ _____
(подпись) (Ф.И.О)

Члены комиссии

_____ _____
(подпись) (Ф.И.О)

_____ _____
(подпись) (Ф.И.О)

_____ _____
(подпись) (Ф.И.О)

М. П.

Приложение 2. Журнал регистрации администраторов безопасности и пользователей

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

Приложение 3. Журнал пользователя сети

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

Индекс

Ш

Э

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