П-274/2023

Министерство образования и науки Самарской области
ГБПОУ «ТК им. Н.Д. Кузнецова»

СОГЛАСОВАНО
Протокол заседания Совета Учреждения
от 31.05.2023г. № 23

Протокол заседания Совета обучающихся Учреждения
от 31.05.2023г. № 23

Протокол заседания Совета родителей Учреждения
от 31.05.2023г. № 23

УТВЕРЖДАЮ
Директор
ГБПОУ «ТК им. Н.Д. Кузнецова»
_____А.Н. Сакеев
«31» мая 2023г.

Приказ № 347 о/д от 31.05.2023

О=ГБПОУ «ТК им. Н.Д. Кузнецова», CN =Сакеев А.Н., E= poo_tkk_su@samara.edu.ru 009939dcd2bdaa96fe 2023.06.07 10:40:46 +04'00'

Положение об организации и проведении работ по обеспечению безопасности конфиденциальной информации с использованием средств криптографической защиты информации в ГБПОУ «ТК им. Н.Д. Кузнецова»

1. Общие положения.

1.1. Положение разработано в целях организации и проведении работ по обеспечению безопасности конфиденциальной информации с использованием средств криптографической защиты в государственном бюджетном профессиональном образовательном учреждении «Технологический колледж имени Н.Д. Кузнецова» (далее – ГБПОУ «ТК им. Н.Д. Кузнецова»).

1.2. Настоящее положение разработано для практического применения пользователями средств криптографической защиты информации (далее – СКЗИ) в ГБПОУ «ТК им. Н.Д. Кузнецова» на основании приказа ФАПСИ РФ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.3. В ГБПОУ «ТК им. Н.Д. Кузнецова» определяются должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СКЗИ.

1.4. В ГБПОУ «ТК им. Н.Д. Кузнецова» разрабатываются нормативные и распорядительные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ.

2. Термины и определения.

В настоящем положении применены следующие термины с соответствующими определениями:

• ***Средства криптографической защиты конфиденциальной информации,*** сертифицированные ФСБ, именуются – СКЗИ. К СКЗИ относятся криптографические алгоритмы преобразования информации, программные средства, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи включая СКЗИ, защиту от несанкционированного доступа к информации и навязывания ложной информации, включая средства имитозащиты и «электронной подписи».

• ***Пользователи СКЗИ*** – физические и юридические лица, непосредственно допущенные к работе с СКЗИ.

• ***Криптографический ключ (криптоключ)*** – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

• ***Ключевая информация*** - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

• ***Ключевой носитель*** - физический носитель определенной структуры (дискета), предназначенный для размещения на нем ключевой информации.

• ***Ключевой документ*** - физический носитель определенной структуры, содержащий ключевую информацию, а при необходимости - контрольную, служебную и технологическую информацию.

• ***Компрометация криптоключей*** – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

3. Порядок обращения с конфиденциальной информацией.

3.1. При работе с конфиденциальной информацией сотрудники, допущенные к самостоятельной работе с СКЗИ, обязаны соблюдать следующие правила:

• информация, полученная сотрудниками при регистрации пользователя, является конфиденциальной и не подлежит разглашению третьим лицам;

• конфиденциальная информация, полученная сотрудниками, в результате выполнения должностных обязанностей в процессе работы с СКЗИ, должна сохраняться в тайне;

• содержание закрытых ключей СКЗИ и ключевых документов должно сохраняться в тайне;

• носители ключевой информации, ключевые документы и инсталлирующие СКЗИ носители должны храниться в шкафах (ящиках, хранилищах) индивидуального пользования, учтённых в соответствующем журнале учета сейфов, металлических шкафов, спецхранилищ и ключей от них в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.2. Не допускается:

• разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер; вставлять ключевой носитель в ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.), а также в дисководы других ПЭВМ;

• записывать на ключевом носителе постороннюю информацию; вносить какие-либо изменения в программное обеспечение СКЗИ и ключевую информацию; модифицировать содержимое ключевых носителей; использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования; снимать несанкционированные копии с ключевых носителей; знакомить кого-либо с содержанием ключевых носителей или передавать кому-

либо ключевые носители.

4. Требования по размещению СКЗИ и режиму охраны.

4.1. Помещения, в которых размещаются программно-технические средства со встроенными СКЗИ, являются спецпомещениями и должны обеспечивать конфиденциальность проводимых работ.

4.2. Размещение спецпомещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств.

4.3. Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

4.4. Входные двери спецпомещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время.

4.5. Окна и двери спецпомещений, как правило, оборудуются охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией.

4.6. Размещение технических средств в спецпомещениях должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна.

4.7. Системные блоки ПЭВМ с СКЗИ оборудуются средствами контроля вскрытия (опломбируются).

4.8. Ремонт и/или последующее использование системных блоков не в целях применения СКЗИ осуществляется после удаления с них программного обеспечения СКЗИ.

5. Требования по обеспечению безопасности СКЗИ и ключевой информации.

5.1. Ключевые и инсталляционные носители с программным обеспечением СКЗИ берутся на поэкземплярный учет в выделенных для этих целей журналах поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов. Учет и хранение ключевых носителей поручается ответственному за эксплуатацию СКЗИ. Для хранения ключевых носителей выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации.

5.2. Хранение ключевых и инсталляционных носителей с ПО СКЗИ допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

5.3. Рабочие (актуальные) и резервные ключевые носители хранятся раздельно, с обеспечением условия невозможности их одновременной компрометации.

6. Порядок допуска к самостоятельной работе с СКЗИ.

6.1. К самостоятельной работе с СКЗИ допускаются лица, принятые на работу в ГБПОУ «ТК им. Н.Д. Кузнецова» в соответствии с распоряжением министра на основании заключенных с ними трудовых договоров и назначенные на должности, выполнение обязанностей по которым связано с изготовлением, хранением и использованием СКЗИ.

6.2. Сотрудники допускаются к самостоятельной работе с СКЗИ после их специальной подготовки (обучения) по утвержденным программам по правилам работы с СКЗИ, не содержащей сведений, составляющих государственную тайну и сдачи зачета на допуск к самостоятельной работе с СКЗИ. Документом, подтверждающим должную специальную подготовку допускаемого и возможность его допуска к самостоятельной работе с СКЗИ является заключение к самостоятельной работе с СКЗИ, составленное комиссией ГБПОУ «ТК им. Н.Д. Кузнецова» (Приложение № 1 к настоящему Положению), на основании принятого зачета по программе подготовки (обучения).

6.3. Программа подготовки к самостоятельной работе с СКЗИ (Приложение № 2 к

настоящему Положению) содержит:

- ознакомление с нормами действующего законодательства Российской Федерации, регулирующими отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; защите информации, прав субъектов, участвующих в информационных процессах и информатизации; использовании электронной подписи в электронных документах; ответственности за нарушение указанных норм;
- ознакомление с нормативными актами органов государственного управления Российской Федерации, определяющими порядок разработки, производства, реализации, использования СКЗИ; регламентирующими вопросы взаимодействия участников информационного обмена с использованием СКЗИ; изучение должностных инструкций, положений о структурных подразделениях, других локальных нормативных актов ГБПОУ «ТК им. Н.Д. Кузнецова» по вопросам производственной деятельности, связанной с хранением и использованием СКЗИ; изучение эксплуатационно-технической документации на СКЗИ; приобретение практических навыков выполнения работ, предусмотренных обязанностями по занимаемой должности.

6.4. Методика подготовки к сдаче зачета на допуск к самостоятельной работе с СКЗИ должна предусматривать формы самостоятельного изучения и освоения программного материала сотрудником.

6.5. Пользователи, допущенные к работе с СКЗИ, регистрируются в журнале учета обучения пользователей СКЗИ.

Положение вступает в силу с момента его утверждения.

В случае необходимости в Положение могут вноситься изменения и дополнения по согласованию с Советом учреждения.

Разработчик:
заместитель директора по общим вопросам

_____/ Ю.Ю. Алексеев /

П-274/2023

Приложение № 1

УТВЕРЖДАЮ
Директор
ГБПОУ «ТК им. Н.Д. Кузнецова»

_____А.Н. Сакеев
«__»_____20___г.

ЗАКЛЮЧЕНИЕ
о допуске к самостоятельной работе
со средствами криптографической защиты информации

Место работы: _____
Должность: _____
Фамилия, имя, отчество: _____
_____

с «____»_____20____г. по «_»_____20____г.

в соответствии с программой, утвержденной приказом ГБПОУ «ТК им. Н.Д. Кузнецова» № _____ от __.__.20__г., прошел(ла) подготовку по правилам работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну, количество часов – 5, и прошел(ла) тестирование_____, результат по итогам тестирования –_____.

По решению комиссии по допуску пользователей к самостоятельной работе с СКЗИ _____допущен(а) / не допущен(а) к самостоятельной работе со средствами криптографической защиты информации.

Председатель комиссии:

_____ подпись Фамилия И.О.

Члены комиссии:

_____ подпись Фамилия И.О.

_____ подпись Фамилия И.О.

_____ подпись Фамилия И.О.

_____ подпись Фамилия И.О.

«_____»_____20___г.

П-274/2023

Приложение № 2

УТВЕРЖДАЮ
Директор
ГБПОУ «ТК им. Н.Д. Кузнецова»

_____А.Н. Сакеев
«31» мая 2023г.

Приказ № 347 о/д от 31.05.2023

ПРОГРАММА
обучения сотрудников ГБПОУ «ТК им. Н.Д. Кузнецова» по правилам работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну

Самара
2023г.

1. Общие положения.

1.1. Настоящая программа разработана в соответствии с требованиями Инструкции «Об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации (далее – СКЗИ) с ограниченным доступом, не содержащих сведений, составляющих государственную тайну.

1.2. Программа предназначена для обучения пользователей СКЗИ государственного бюджетного профессионального образовательного учреждения «Технологический колледж имени Н.Д. Кузнецова» (далее – ГБПОУ «ТК им. Н.Д. Кузнецова»).

2. Темы занятий.

2.1. Организация защиты информации при использовании СКЗИ.

2.1.1. Нормативные правовые акты, регламентирующие правила работы со СКЗИ, не содержащей сведений, составляющих государственную тайну:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением председателя Гостехкомиссии России от 30.03.1992г.);
- нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденный приказом Гостехкомиссии России от 30.08.2002 № 282;
- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ РФ от 13.06.2001 № 152.

2.1.2. Базовые требования к организации защиты информации с использованием средств криптографической защиты.

Для защиты информации в органах исполнительной власти (далее – ОИВ) необходим целый комплекс мероприятий по ее защите. Это:

- установление особого режима конфиденциальности;
- ограничение доступа к конфиденциальной информации;
- использование организационных мер и технических средств защиты информации;
- осуществление контроля за соблюдением установленного режима конфиденциальности.

Конкретное содержание указанных мероприятий для каждого отдельно взятого ОИВ может быть различным по масштабам и формам. Это зависит в первую очередь от

деятельности ОИВ, от объемов конфиденциальной информации и степени ее значимости. Существенным является то, что весь перечень указанных мероприятий обязательно должен планироваться и использоваться с учетом особенностей функционирования информационной системы ОИВ.

2.1.3. Установление особого режима конфиденциальности.

Установление особого режима конфиденциальности направлено на создание условий для обеспечения физической защиты носителей конфиденциальной информации.

Как правило, установление особого режима конфиденциальности включает в себя:

- организацию охраны помещений, в которых содержатся носители конфиденциальной информации;
- установление режима работы в помещениях, в которых содержатся носители конфиденциальной информации;
- установление пропускного режима в помещения, содержащие носители конфиденциальной информации;
- закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;
- установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);
- организацию ремонта технических средств обработки конфиденциальной информации;
- организацию контроля за установленным порядком.

2.1.4. Условия соблюдения особого режима конфиденциальности.

Требования к выполнению установленного режима конфиденциальности оформляются в виде организационно-распорядительных документов и доводятся для ознакомления до сотрудников ГБПОУ «ТК им. Н.Д. Кузнецова».

Ограничение доступа к конфиденциальной информации способствует созданию наиболее эффективных условий сохранности конфиденциальной информации. Необходимо четко определять круг сотрудников, допускаемых к конфиденциальной информации, к каким конкретно сведениям им разрешен доступ и полномочия сотрудников по доступу к конфиденциальной информации.

Традиционно для организации доступа к конфиденциальной информации использовались организационные меры, основанные на строгом соблюдении сотрудниками процедур допуска к информации, определяемых соответствующими инструкциями, приказами и другими нормативными документами.

Однако с развитием компьютерных систем эти меры перестали обеспечивать необходимую безопасность информации. Появились и в настоящее время широко применяются специализированные программные и программно-аппаратные средства защиты информации, которые позволяют максимально автоматизировать процедуры доступа к информации и обеспечить при этом требуемую степень ее защиты.

2.1.5. Организация контроля за соблюдением установленного режима конфиденциальности.

Осуществление контроля за соблюдением установленного режима конфиденциальности предусматривает проверку соответствия организации защиты информации установленным требованиям, а также оценку эффективности применяемых мер защиты информации.

Контроль осуществляется в виде плановых и внеплановых проверок силами своих сотрудников или с привлечением других организаций, которые специализируются в этой области. А также проверки осуществляются на уровне межведомственного – государственного контроля организациями, уполномоченными в сфере безопасности информации.

По результатам проверок специалистами по защите информации проводится

необходимый анализ с составлением отчета, который включает:

- вывод о соответствии проводимых на предприятии мероприятий установленным требованиям;
- оценка реальной эффективности применяемых на предприятии мер защиты информации и предложения по их совершенствованию.

2.1.6. Необходимость создания органов защиты информации.

Для обеспечения и реализации перечисленных мероприятий (контроль, планирование и т.д.) потребуется создание соответствующих органов защиты информации. Эффективность защиты информации во многом будет определяться тем, насколько правильно выбрана структура органа защиты информации и квалифицированы его сотрудники.

Органы защиты информации представляют собой самостоятельные подразделения, однако на практике часто используется назначение одного или нескольких из штатных специалистов организации, ответственных за обеспечение защиты информации.

Однако такая форма оправдана в тех случаях, когда объем необходимых мероприятий по защите информации небольшой и создание отдельного подразделения экономически не выгодно.

2.1.7. Средства защиты информации при передаче ее по каналам связи.

С развитием сетевых технологий появился новый тип средств защиты – межсетевые экраны (firewalls), которые обеспечивают решение таких задач, как защита подключений к внешним сетям, разграничение доступа между сегментами корпоративной сети, защита корпоративных потоков данных, передаваемых по открытым сетям.

Защита информации при передаче ее по каналам связи осуществляется средствами криптографической защиты (далее – СКЗИ). Характерной особенностью этих средств является то, что они потенциально обеспечивают наивысшую защиту передаваемой информации от несанкционированного доступа к ней. Помимо этого, СКЗИ обеспечивают защиту информации от модификации (использование цифровой подписи и имитовставки).

Как правило, СКЗИ функционируют в автоматизированных системах в составе средств разграничения доступа, как функциональная подсистема для усиления защитных свойств последних.

Хотя имеется достаточно большое количество СКЗИ в виде самостоятельных продуктов, решающих конкретные задачи криптографической защиты.

2.2. Требования к ОИВ по управлению ключевой информацией СКЗИ.

2.2.1. Хранение ключевых носителей.

Личные ключевые носители пользователей рекомендуется хранить в сейфе.

Пользователь несет персональную ответственность за хранение личных ключевых носителей.

При наличии в ОИВ, эксплуатирующей СКЗИ, ответственного пользователя СКЗИ (далее 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.

2.2.2. Сроки действия ключей.

Сроки действия пользовательской ключевой информации, как правило, не должны превышать 1 год 3 месяца.

Сроки действия системной ключевой информации (например, выдающего центра системы управления сертификатами), как правило, не должны превышать 3-5 лет.

2.2.3. Уничтожение ключевой информации на ключевых носителях.

Ключевая информация на ключевых носителях, срок действия которой истек, уничтожается согласно требованиям технической документации на СКЗИ в основном путем переформатирования (очистки).

Ключевые носители могут быть использованы в дальнейшем только при условии записи на них новой ключевой информации.

2.2.4. Учет пользовательской ключевой информации.

В ОИВ должен вестись "Журнал учета квалифицированных ключей", в которых следует вносить следующую информацию:

- Ф.И.О. лица, производящего запись;
- дата создания ключа;
- идентификаторы ключа (таблицы ключей) (например: серия, номер, комплект и т.п.);
- дата передачи/получения ключа;
- Ф.И.О. получателя/отправителя ключа;
- номер и дата акта о передаче ключа или подпись получателя;
- номер и дата акта об уничтожении ключа;
- запись о компрометации ключа.

2.2.5. Рекомендации по размещению технических средств СКЗИ.

При размещении технических средств СКЗИ, следует руководствоваться следующими рекомендациями:

- 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.
- Рекомендуется не использовать в помещении, где размещены рабочие места с установленным СКЗИ, радиотелефоны и другую радиоаппаратуру.
- Должны выполняться требования политики безопасности, принятой в организации в области размещения технических средств, обрабатывающих конфиденциальную информацию.

2.2.6. Требования к программному и аппаратному обеспечению.

На технических средствах, оснащенных СКЗИ, должно использоваться только лицензионное программное обеспечение (далее – ПО), либо ПО, сертифицированное ФСБ России. Указанное ПО не должно содержать средств разработки и отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование СКЗИ. В любом случае ПО не должно содержать в себе возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- использовать недокументированные фирмами разработчиками функции.

На персональной электронно-вычислительной машине (далее – ПЭВМ) одновременно может быть установлена только одна разрешенная ОС.

В BIOS ПЭВМ должны быть определены установки, исключающие возможность загрузки иной операционной системы, отличной от установленной на жестком диске. Отключается возможность загрузки с гибкого диска, привода CD/DVD-ROM и прочие нестандартные виды загрузки ОС (за исключением случаев, предусмотренных при эксплуатации ПО, использующего СКЗИ), включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой грузки ОС (кроме автономных ПЭВМ).

Средствами BIOS должна быть исключена возможность отключения пользователями PCI устройств при использовании программного аппаратного комплекса (далее – ПАК) защиты от несанкционированного доступа (далее – НСД), устанавливаемых в PCI разъем.

Вход в BIOS ПЭВМ должен быть защищен паролем с длиной не менее 6 символов.

2.2.7. Организационные меры защиты информации от НСД.

При использовании СКЗИ должны соблюдаться следующие организационные меры:

- право доступа к рабочим местам с установленным ПО СКЗИ предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе СКЗИ;
- запрещается осуществление несанкционированного Администратором безопасности копирования ключевых носителей;
- запрещается разглашение содержимого ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер;
- запрещается использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ, либо использовать ключевые носители на посторонних ПЭВМ;
- запрещается запись на ключевые носители посторонней информации;
- на технических средствах, оснащенных СКЗИ, должно использоваться только лицензионное программное обеспечение фирм-производителей;
- на ПЭВМ, оснащенных СКЗИ, 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. Необходимо исключить попадание в систему программ, позволяющих, пользуясь ошибками ОС, получать привилегии администратора;
- должен быть исключен несанкционированный доступ посторонних лиц в помещения, в которых установлены технические средства СКЗИ, по роду своей деятельности, не являющихся персоналом, допущенным к работе в указанных помещениях;
- запрещается оставлять без контроля вычислительные средства, которые эксплуатируются после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки;
- администратором безопасности должно быть проведено опечатывание системного блока с установленным СКЗИ, исключающее возможность несанкционированного изменения аппаратной части рабочей станции;
- 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;
- при использовании СКЗИ 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;
- 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;
- средствами BIOS должна быть исключена возможность отключения пользователями PCI устройств при использовании ПАК защиты от НСД, устанавливаемых в PCI разъемах;

• вход в BIOS ПЭВМ должен быть защищен паролем. Пароль для входа в BIOS должен быть известен только администратору безопасности;

• средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты;

• при загрузке ОС должен производиться контроль целостности программного обеспечения, входящего в состав СКЗИ, самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ;

• должно производиться физическое затирание содержимого удаляемых файлов;

• должны быть реализованы организационно-технические меры защиты;

• должны быть внесены изменения в системном реестре ОС Windows, выполнены дополнительные настройки ОС в соответствии с правилами пользования.

2.2.8. Правила безопасности функционирования рабочих мест со встроенным СКЗИ:

• личные ключевые носители пользователей рекомендуется хранить в сейфе;

• рабочие места, на которые установлены СКЗИ, должны быть аттестованы комиссией. Результаты работы комиссии отражаются в " Акте установки средств криптографической защиты информации, ввода в эксплуатацию и закрепления их за ответственными лицами»;

• 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;

• должностные инструкции администратора безопасности (его заместителя) и ответственного исполнителя должны учитывать требования настоящих Правил;

• 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;

• администратор безопасности должен периодически (не реже одного раза в два месяца) проводить контроль целостности и легальности установленных копий ПО на всех ПЭВМ со встроенной СКЗИ с помощью программ контроля целостности;

• в случае обнаружения «посторонних» (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на ПЭВМ должна быть прекращена.

• По данному факту должно быть проведено служебное расследование постоянно действующей комиссией по допуску пользователей к самостоятельной работе при помощи СКЗИ (далее – комиссия) в присутствии пользователя, на ПЭВМ которого произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения;

• 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;

• при каждом включении рабочей станции с установленным СКЗИ необходимо проверять сохранность печатей системного блока и разъемов рабочей станции;

• пользователь должен запускать только те приложения, которые разрешены администратором безопасности; на ПЭВМ должна быть установлена только одна ОС;

• ПО, установленное на ПЭВМ, не должно иметь встроенных средств разработки и отладки программ;

• должны быть приняты меры по исключению вхождения пользователей в режим конфигурирования BIOS (например, с использованием парольной защиты);

• должна быть исключена возможность работы на ПЭВМ, если во время начальной загрузки не проходят встроенные тесты;

• ПЭВМ, обеспечивающие удаленный вход пользователей из глобальной сети, (например, RAS сервер) не должны использовать ПО СКЗИ;

• пароли, назначаемые пользователям, должны отвечать требованиям соответствующих инструкции и нормативных документов ОИВ;

• защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем, администраторами безопасности или контролирующими органами.

2.3. Криптография

2.3.1. Криптография в современном мире.

Поскольку ПЭВМ оперирует с информацией в одном из видов исчисления (битовая, восьмеричная, шестнадцатеричная, десятичная и т.п., это значит, что к информации могут быть применены математические операции функции. На этом и основываются современные системы криптографии или КРИПТОСИСТЕМЫ.

Криптосистемы по методам работы ключей и алгоритмов, криптосистемы имеют разделение на симметричные, ассиметричные и гибридные. В свою очередь, ассиметричные криптоалгоритмы делятся на блочные, потоковые и комбинированные.

• Симметричные криптосистемы.

• Принцип работы симметричных криптосистем (правильнее в данном случае назвать их криптоалгоритмами), основан на использовании определенных операций с информацией на одной стороне или абсолютно одинаковых (в прямом и обратном порядке) или с маленькими различиями (например, с разными методами разделения ключа).

• Блочные, потоковые и гибридные системы.

• Самое общепринятое деление криптоалгоритмов организовано по их методу обработки информации.

• Блочные криптоалгоритмы.

• Делят сообщение целиком на отдельные блоки равной длины и производят операции с каждым блоком.

• Потоковые криптоалгоритмы.

Обрабатывают поток информации по мере его поступления. При этом поток не имеет начала или конца для криптосистемы.

2.3.2. Разновидности ключей.

Еще одно деление криптоалгоритмов обычно основано на принципе использования ключа или ключей. При этом есть кардинальная разница между симметричным криптоалгоритмом и симметричным ключом. Симметричный ключ является всего лишь одним из вариантов реализации симметричного криптоалгоритма, хотя данный вариант является самым распространенным, есть и другие реализации использования ключей. Рассмотрим самые часто встречающиеся.

Ключом в криптографии называется некая цифровая последовательность, файл или фраза, при помощи которой можно либо сразу произвести дешифрование (декриптование) шифрованного сообщения, либо, преобразовав ключ, произвести данное действие.

Разновидность симметричного ключа предполагает использование для процессов шифрования и расшифрования (дешифрования) одинакового ключа.

Основной минус:

• Ключ не может быть передан по небезопасным каналам, поскольку является компрометирующим фактором безопасности.

Плюсы:

• Широкая реализация разновидностей решений и скорость криптопреобразования информации.

При использовании первичного и вторичного ключей подразумевают систему, при которой первичный ключ является шифрующим, а вторичный расшифровывающим. В этом случае во время шифрования закладывается некий фактор, который необходим, чтобы

преобразовать первичный ключ во вторичный.

Разновидность первичного и вторичного ключей предполагает использование для процессов шифрования и расшифрования (дешифрования) двух разных ключей, причем второй может быть получен из первого при использовании того же фактора преобразования, который применялся при шифровании.

Основной минус:

- Фактор преобразования должен быть каким-то образом передан второму абоненту или вычислен им самостоятельно. Именно фактор преобразования является слабым местом данной разновидности криптосистемы.

Плюсы:

- Дополнительная безопасность путем разделения функций первичного и вторичного ключей. Передача первичного ключа по открытым каналам не несет прямой угрозы конфиденциальности сообщения.

При оценке криптоалгоритмов, обычно как основное качество, учитывают их возможность противостоянию взлому и криптоанализу.

Взлом-процесс прямого перебора ключей с целью найти тот, который сможет расшифровать шифрованное сообщение. При этом злоумышленник должен иметь шифрованное сообщение, знать алгоритм, с которым оно шифровано и иметь программные и аппаратные ресурсы для запуска подбора ключа или пароля. При этом облегченным взломом называется взлом, когда злоумышленнику известен хотя бы один фактор относительно ключа (например, длина ключа или пароля, какие в нем могут быть символы и т.п.).

Криптоанализ же, в отличие от взлома, предполагает наличие неких двух компонентов для проведения их математического сопоставления с целью выявления взаимосвязей.

Криптоанализ делят на линейный и дифференциальный.

Линейным криптоанализом называется процесс сравнения нешифрованного и шифрованного сообщения или его частей.

Дифференциальный криптоанализ состоит в выявлении взаимосвязи между шифрованным сообщением (или его частью) и ключом шифрования.

Распространенные алгоритмы:

- AES (англ. Advanced Encryption Standard) – американский стандарт шифрования;
- ГОСТ 28147-89 – отечественный стандарт шифрования данных;
- DES (англ. Data Encryption Standard) – стандарт шифрования данных в США до AES;
- 3DES (Triple-DES, тройной DES);
- RC6 (Шифр Ривеста);
- Twofish;
- IDEA (англ.International Data Encryption Algorithm);
- SEED – корейский стандарт шифрования данных;
- Camellia – сертифицированный для использования в Японии шифр;
- CAST (по инициалам разработчиков Carlisle Adams и Stafford Tavares);
- XTEA – наиболее простой в реализации алгоритм.

2.4. Электронная подпись

При постепенном переводе данных в электронный вид, встал вопрос не только о сохранении конфиденциальности документа (применением шифрования), целостности документа (применением хэширования), но также и привязке документа к человеку и однозначное отношение этого человека к документу. Эти требования к электронному документообороту носят название подтверждение авторства и невозможность отказа от авторства. Именно их реализует электронная подпись (далее – ЭП).

В соответствии с Федеральным законом «Об электронной подписи» от 06 апреля 2011 года № 63-ФЗ (далее 63-ФЗ) используются следующие основные понятия:

- электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом

связана с такой информацией и которая используется для определения лица, подписывающего информацию;

- сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром (далее – УЦ), либо доверенным лицом УЦ и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;
- квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) – сертификат ключа проверки электронной подписи, выданный аккредитованным УЦ или доверенным лицом аккредитованного УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее – уполномоченный федеральный орган);
- владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;
- ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи;
- ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее – проверка электронной подписи);
- удостоверяющий центр – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;
- средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;
- участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;
- корпоративная информационная система – информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

Также можно сказать, что ЭП – реквизит электронного документа, обеспечивающий сохранение авторства и неизменности документа при его пересылке и ознакомлении, а также (как дополнительная функция), возможность применения системы разграничения доступа к документу и его использования на уровне пользователей. Согласно законодательным актам, ЭП равносильна собственноручной подписи владельца сертификата ключа проверки ЭП на бумажном документе при соблюдении некоторых простых условий.

Электронная подпись – это эффективное средство защиты информации от модификации, которое переносит свойства реальной подписи под документом в область электронного документооборота. В основу ЭП положены такие криптографические методы, как асимметричное шифрование и хэш-функции. Процесс ЭП использует криптографические преобразования для создания самого ЭП, несущего дополнительную информацию об авторе, времени подписи и иногда о назначении подписи (зависит от клиентской среды документооборота).

ЭП в своем составе использует хэширование. Фактически, в составе ЭП содержится как минимум два хэш-отпечатка, один предназначен для защиты целостности файлов в подписываемом сообщении, второй (называемый решающим), защищает сведения ЭП от подделки.

ЭП может содержаться в одном из нескольких видов. Чаще всего различают Первичную, Дополняющую и Заверяющую ЭП:

- Первичная ЭП, которой заверяется и защищается от изменения содержимого самого

сообщения. Первичная подпись может быть только одна. Другие виды ЭП не могут находится в документе без первичной ЭП.

- Дополняющая ЭП, которой дополнительно заверяется содержимое, но, например, другим пользователем или сертификатом. Дополняющая подпись существует только при наличии Первичной подписи, при этом доверие первичной подписи не обязательно. Дополняющая подпись может отсутствовать в документе, может быть одна или сразу несколько.
- Заверяющая ЭП, которая заверяет не содержимое, а одну из подписей (Первичную или одну из дополняющей). При этом не обязательно доверие содержимому документа, но обязательно доверие к подписи, которая заверяется. Заверяющая подпись может отсутствовать, либо присутствовать на любом уровне, также заверяющих подписей может быть несколько.

В соответствии с 63-ФЗ существуют следующие виды электронных подписей:

1. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

2. Усиленная неквалифицированная электронная подпись (далее – неквалифицированная электронная подпись). Неквалифицированной электронной подписью является электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

3. Усиленная квалифицированная электронная подпись (далее – квалифицированная электронная подпись). Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с 63-ФЗ.

При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи может быть обеспечено без использования сертификата ключа проверки электронной подписи.

Выделяются два формата ЭП:

1. CAdES BES. Этот вид является минимальным форматом ЭП, которая может вырабатываться подписывающей стороной. Сам по себе этот формат не включает достаточного набора информации для обеспечения возможности проверки подписи в течение длительного промежутка времени.

2. CAdES Explicit Policy-based Electronic Signatures (CAdES EPES) – расширяет определение ЭП для согласования с заданным регламентом.

В число дополнений входят:

- штамп времени - подписанный ЭП документ, которым служба штампов времени удостоверяет, что в указанный момент времени ей было предоставлено значение хеш-функции от другого документа. Само значение хеш-функции также указывается в штампе времени. Предоставляется службой штампов времени (TSA), компонентом УЦ, обладающим точным и надежным источником времени и предоставляющим услуги по созданию штампов времени;
- цепочки сертификатов до доверенного УЦ и OCSP-ответов. На эти данные также

получается штамп времени, подтверждающий их целостность в момент проверки.

Если в подпись будут вложены все доказательства, необходимые для проверки ее подлинности, то будет обеспечена оффлайновая проверка подлинности вне зависимости от того, существует ли в момент проверки тот или иной УЦ, выдавший в свое время сертификат подписи. Такая подпись, в которую будет вложена вся необходимая для последующей проверки информация, может храниться неограниченно долго, если будет обеспечена ее целостность.

ЭП участвует в общей информационной системе или применительно к электронному документообороту (далее – ЭДО) или как дополнительное средство обеспечения безопасности данных.

Для нормального функционирования системы ЭП, должны присутствовать следующие участники системы:

- УЦ;
- операторы ключевой системы, пользователи, на компьютерах которых присутствует клиентское ПО для создания и проверки ЭП, а также носители, на которых сохранены индивидуальные наборы ключей.

2.5. Крипто Про CSP.

Крипто Про CSP- криптопровайдер реализует следующие алгоритмы:

- ГОСТ 28147-89 – симметричное шифрование;
- ГОСТ Р 34.11-94 - функция хэширования;
- ГОСТ Р 34.10-2001 - электронная подпись, асимметричное шифрование;
- ГОСТ Р 34.10-2012 – электронная подпись, функция хеширования;
- ГОСТ Р 34.12-2015 («Кузнечик» — начиная с 5.0 R2);
- ГОСТ 28147-89, AES (128/192/256), 3DES, 3DES-112, DES, RC2, RC4.

Сертификат ФСБ РФ подтверждает, что реализованные алгоритмы и внутренние средства защиты СКЗИ Крипто Про CSP позволяют защищать с его помощью конфиденциальную информацию.

К средствам защиты государственной тайны предъявляются более высокие требования, поэтому средствами СКЗИ Крипто Про CSP НЕ ДОПУСКАЕТСЯ защищать информацию, составляющую государственную тайну.

Криптографические алгоритмы ГОСТ Р 34.11-94 (функция хэширования) и ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (ЭП), реализованные в СКЗИ Крипто Про CSP, а также сертификат ФСБ, позволяют использовать его в соответствии с требованиями 63-ФЗ как сертифицированное средство ЭП для авторизации, контроля целостности и обеспечения юридической значимости электронных документов.

Симметричное шифрование и имитозащита по ГОСТ 28147-89 позволяют использовать Крипто Про CSP для обеспечения конфиденциальности и контроля целостности информации.

По протоколу Диффи-Хеллмана на основе асимметричного алгоритма ГОСТ Р 34.10-2001 может быть создан общий секрет, что даёт возможность выработки общего ключа симметричного шифрования на основе асимметричных ключей с аутентификацией сторон. Эта функциональность позволяет реализовать протокол асимметричного шифрования с ключами ГОСТ Р 34.10-2001.

Крипто Про CSP поддерживает формат сертификатов открытых ключей X.509 и реализует все необходимые алгоритмы для установления защищённого соединения по протоколу TLS с аутентификацией одной или двух сторон.

Созданное таким образом соединение обеспечивает должный уровень защиты для передачи по каналу связи конфиденциальной информации.

Внутренние средства защиты Крипто Про CSP обеспечивают контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированного изменения или от нарушения правильности функционирования.

Это необходимо для обеспечения требуемого уровня защиты обрабатываемой

информации и криптографических ключей.

Крипто Про CSP реализует процедуры управления криптографическими ключами, такие как создание, копирование и удаление. Таким образом, Крипто Про CSP может использоваться для управления ключевыми элементами системы в целях реализации регламента средств защиты.

Требуемый уровень защиты ключей обеспечивается только при работе с ними штатными средствами Крипто Про CSP. Например, удалять ключ путём форматирования диска нельзя.

Крипто Про CSP 4.0:

- Текущая установленная сертифицированная версия;
- Ключевые изменения по сравнению с 3.6: работа на Windows 2008/W7/W10/W11, на процессорах x64, расширен перечень поддерживаемых UNIX-платформ;
- Поддерживается установка на КПК и смартфоны.

Все версии Крипто Про CSP совместимы по форматам сообщений. Например, можно установить TLS-соединение с клиента версии 3.0 на сервер с версией 4.0. Аналогично, электронное письмо, зашифрованное и подписанное в версии 4.0. будет корректно расшифровано и проверено в версии 2.0.

Поддерживается обратная совместимость ключевых контейнеров. Ключи, созданные в более ранних версиях Крипто Про CSP могут использоваться в более поздних версиях, но не наоборот.

Размеры ключей электронной подписи:

- закрытый ключ –256 бит;
- открытый ключ –512 бит.
- Размеры ключей, используемых при шифровании:
- закрытый ключ –256 бит;
- открытый ключ –512 бит;
- симметричный ключ –256 бит.

Указанные размеры ключей определены соответствующими ГОСТами и не изменяются. Открытый ключ длиной 512 бит считается в настоящее время достаточным для асимметричных алгоритмов на эллиптических кривых, а размер закрытого ключа определяется размером открытого ключа. Симметричный ключ размером 256 бит также считается достаточным для обеспечения высокого уровня защиты.

Симметричные ключи ГОСТ 28147-89 вырабатываются либо для одного сеанса связи, либо для защиты одного сообщения, и поэтому передаются и хранятся вместе с этим сообщением (обязательно в защищённом виде). Таким образом, хранение симметричных ключей на специальных носителях не требуется.

СКЗИ Крипто Про CSP может сохранять закрытые ключи ГОСТ Р 34.10-2001 на различных ключевых носителях. Ключ на ключевом носителе может быть защищён паролем. Поддерживаются следующие типы носителей:

- Съёмные диски: USB флеш-накопитель и т.п.;
- Смарт-карты и USB-токены;
- Идентификаторы (таблетки) Touch Memory;
- Жёсткий диск или реестр Windows.

2.6. Хранение ключевых носителей.

Личные ключевые носители пользователей рекомендуется хранить в сейфе.

Пользователь несет персональную ответственность за хранение личных ключевых носителей.

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

в его личном сейфе.

При хранении ключей на жёстком диске или в реестре Windows требования по хранению личных ключевых носителей распространяются на ПЭВМ. При использовании реестра требования сохраняются в том числе и после удаления ключей из реестра.

Настоятельно рекомендуется использовать парольную защиту при хранении ключей в реестре или на жёстком диске.

2.7. Сроки жизни ключей.

В руководстве по эксплуатации СКЗИ Крипто Про CSP установлены следующие сроки действия ключей:

- максимальный срок действия закрытых ключей шифрования и ЭП –1 год 3 месяца;
- максимальный срок действия открытых ключей шифрования –1 год 3 месяца;
- максимальный срок действия открытых ключей ЭП –30 лет.

После истечения установленных сроков действия закрытые ключи должны быть уничтожены во избежание неявной компрометации, а открытым ключам не следует доверять.

Обратить внимание на различие сроков действия, закрытого и открытого ключей ЭП. Для создания ЭП закрытый ключ может использоваться 1 год 3 месяца, после чего он должен быть уничтожен, но проверять созданные ЭП с помощью открытого ключа можно в течение 30 лет.

Срок действия открытого ключа дополнительно ограничивается сроком действия сертификата открытого ключа, который устанавливается в соответствии с регламентом выдавшего данный УЦ.