Муниципальное бюджетное дошкольное общеобразовательное учреждение
«Детский сад №6 п.Смидович»

ПРИКАЗ

дата	номер
28.06.2024	38

О мерах по обеспечению защиты информации
при работе с криптографическими средствами

Во исполнение требований Федеральных законов от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», «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» (Приложение к приказу ФАПСИ от 13.06.2001 № 152, зарегистрировано № 2848 от 06.08.2001 Минюста России

ПРИКАЗЫВАЮ:

1. Назначить Филимонову Наталью Владимировну ответственным за работу со средствами криптографической защиты информации (далее - СКЗИ), конфиденциальными сведениями, ключевыми носителями и ключевой документацией
2. Утвердить порядок доступа работников в помещения, в которых установлены средства криптографической защиты информации и хранятся ключевые документы, в рабочее и нерабочее время, а также в нештатных ситуациях (приложение №1)
3. Утвердить инструкцию ответственного за работу с СКЗИ (приложение № 2).
4. Утвердить положение по организации криптографической защиты информации (приложение № 3).
5. Утвердить инструкцию пользователя СКЗИ (приложение № 4).
6. Утвердить политику назначения и смены паролей для автоматизированных рабочих мест с установленными СКЗИ (приложение № 5).
7. Утвердить список пользователей СКЗИ, имеющих право самостоятельного доступ в помещения с установленными СКЗИ (приложение № 6).
8. Журнал учёта обучения пользователей СКЗИ (приложение № 7).
9. Журнал учета опломбирования СКЗИ, а также аппаратных средств, с которыми осуществляется функционирование СКЗИ (приложение №8).
10. Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Приложение № 9).
11. Технический (аппаратный) журнал (Приложение №10).
12. Типовую форму акта установки и ввода в эксплуатацию СКЗИ (приложение №14).
13. Типовую форму акта об уничтожении средств криптографической защиты информации, криптографических ключей, содержащихся на ключевых носителях, и ключевых документов (приложение №15).
14. Работникам согласно списку пользователей СКЗИ, имеющих право самостоятельного доступ в помещения с установленными СКЗИ самостоятельно пройти обучение согласно программе обучения (приложение №16).

15. Ответственному за работу с СКЗИ:

15.1 Поддерживать в актуальном состоянии список пользователей СКЗИ, имеющих право самостоятельного доступ в помещения с установленными СКЗИ.

15.2 После успешного прохождения обучения работников, указанных в п.14 настоящего приказа оформить заключения о допуске к самостоятельной работе со средствами криптографической защиты информации (приложение №18).

15.3 Осуществить опечатывание кабинета со средствами криптографической защиты информации (ViPNet Client, КриптоПро CSP Континент –АП Код Безопасности CSP).

15.4 Завести журналы, указанные в настоящем приказе.

16. Контроль исполнения приказа оставляю за собой.

Заведующий Н.В. Филимонова

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00E719B594F57DA57381EAD5AC67BBA67C
Владелец: Филимонова Наталья Владимировна
Действителен: с 08.09.2023 до 01.12.2024

СОГЛАСОВАНО:
Председатель СТК
МБДОУ «Детский сад №6 п.Смидович»

Н.Г.Дмитрякова

ЖДАЮ:
ощий
/ «Детский сад №6 п.Смидович
лимонова

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00E719B594F57DA57381EAD5AC67BBA67C
Владелец: Филимонова Наталья Владимировна
Действителен: с 08.09.2023 до 01.12.2024

Порядок доступа работников в помещение, в котором ведется обработка информации ограниченного доступа, и расположены средства криптографической защиты информации в
МБДОУ «Детский сад № 6 п. Смидвич»

1. Общие положения

Настоящий порядок доступа работников в помещение МБДОУ»Детский сад № 6 п. Смидович", в котором ведется обработка информации ограниченного доступа, в том числе персональных данных, (далее - Информации) не содержащей сведения, составляющие государственную тайну, и расположены средства криптографической защиты информации разработан в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных», приказом Федерального агентства Правительственной связи и информации при Президенте Российской Федерации 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», приказом Федеральной службы безопасности 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»

Обеспечение безопасности Информации от уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении Информации достигается, в том числе, установлением· правил доступа в помещение, где обрабатывается Информация с использованием и/или без использования средств автоматизации.

Размещение информационных систем (далее - ИС), в которых обрабатывается Информация, должно осуществляться в пределах контролируемых зон, регламентированных эксплуатационной и технической документацией к средствам криптографической защиты информации. Для помещения, в которых обрабатывается Информация (далее - Помещение) и расположены средства криптографической защиты информации (далее - СКЗИ), организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей Информации и средств защиты информации, крипто средств и ключевых документов к ним, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц и просмотра ведущихся там работ.

2. Допуск в помещение, в котором ведётся обработка информации ограниченного доступа

В помещение, где размещены технические средства, позволяющие осуществлять обработку Информации, а также хранятся носители Информации, допускаются только работники, уполномоченные на обработку Информации (в соответствии с приказом об утверждении перечня должностей, допущенных к обработке персональных данных), а также только лица, имеющие право доступа в помещение детского сада, где осуществляется обработка Информации (в соответствии с перечнем лиц, имеющих право доступа в помещение, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой и парольной информации.

При оборудовании помещений должны выполняться требования к размещению, монтажу крипто средств, а также другого оборудования, функционирующего с крипто средствами.

Для помещения, в котором обрабатываются персональные данные , должен быть назначен ответственный за режим безопасности и правильность использования установленных в нем технических средств.

Перечень ответственных за режим безопасности в них утверждает заведующий.

.Нахождение в помещении с ИС лиц, не включенных в перечни доступа возможно только в присутствии работника, уполномоченного на обработку информации в данном помещении. Время нахождения в помещениях ограничивается временем решения вопросов, в рамках которого возникла необходимость пребывания в помещении.

Работники, допущенные к обработке Информации, не должны покидать ЗП, не убедившись, что доступ посторонних лиц к Информации невозможен. Запрещается оставлять материальные носители Информации без присмотра в незапертом помещении.

В помещении, в котором ведется обработка Информации и расположены средства криптографической информации оснащено входной дверью с замком, обеспечения постоянного закрытия дверей ЗП на замок и их открытия только для санкционированного прохода, а также опечатывания ЗП по окончании рабочего дня **.**

В нерабочее время помещение, в котором осуществляется функционирование СКЗИ, должно ставиться на охрану, при этом все окна и двери должны быть надежно закрыты, ключевые документы убраны в запираемые шкафы (сейфы).

3. Допуск в помещение, в котором ведётся обработка информации ограниченного доступа

Для предотвращения просмотра извне окна помещения должно быть защищено шторами или жалюзи.

Окна ЗП, расположенных на первых или последних этажах здании, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в ЗП посторонних лиц, оборудуются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в ЗП.

При утрате ключа от хранилища или от входной двери в помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей. Факт изготовления новых ключей должен быть документально оформлен в виде акта в произвольной форме. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить.

Внутренний контроль за соблюдением порядка доступа в помещение, проводится в порядке, определенном в плане проведения внутреннего контроля соответствия требованиям по защите. Контрольи управление физическим доступом к информационным

системам и средствам криптографической защиты должны предусматривать:

- поддерживание в актуальном состоянии Перечня лиц, имеющих доступ в помещения, в которых расположены технические средства ИС, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах и Перечня лиц, имеющих право доступа в помещение, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой и парольной информации СКЗИ информационных систем , санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещение и сооружение, в которых они установлены - выдача ключей от помещения строго в соответствии с утвержденным перечнем лиц;

В обычных условиях помещение и находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями СКЗИ или ответственным пользователем СКЗИ.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в это помещение посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю СКЗИ. Прибывший ответственный пользователь СКЗИ должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации информации ограниченного доступа и к замене скомпрометированных криптоключей.

Ответственность за соблюдение порядка доступа в помещение, в которых ведется обработка Информации и расположены средства криптографической информации, возлагается на сотрудников, уполномоченных на обработку Информации в детском саду.

В случае нарушения настоящего Порядка работники могут быть привлечены к дисциплинарной и/или иной ответственности в соответствии с законодательством Российской Федерации

Приложение 2

УТВЕРЖДЕНА
Приказом заведующего МБДОУ
«Детский сад № 6 п.Смидович»
Н.В. Филимонова
от 28.06.2024 г. № 38

ИНСТРУКУИЯ
ответственного за работу с СКЗИ

1. Общие положения

1.1. Ответственный за работу с СКЗИ организует и обеспечивает проведение работ по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, при использовании средств криптографической защиты информации.

1.2. Инструкция разработана на основании требований Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», «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» (Приложение к приказу ФАПСИ от 13.06.2001 № 152, зарегистрировано № 2848 от 06.08.2001 Минюста России, далее – Инструкция), Приказа ФСБ России от 10 июля 2014 г. № 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. Ответственный за работу с СКЗИ должны иметь высшее профессиональное образование и практический опыт работы в области криптографической защиты информации, знать законодательство Российской Федерации, нормативные акты и организационно-распорядительные документы «МБДОУ Детский сад №6 п.Смидович» и федеральных органов исполнительной власти, уполномоченных в области безопасности и защиты

информации, а также правила работы с ключевыми носителями и ключевыми документами, применяемыми в эксплуатируемых СКЗИ.

1.4. Мероприятия по обеспечению криптографической защиты информации являются составной частью деятельности по защите информации в «МБДОУ Детский сад №6 п.Смидович» и осуществляются по следующим основным направлениям:

а) осуществление мероприятий по организации передачи информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, с использованием средств криптографической защиты информации (далее – СКЗИ) по сетям связи;

б) обеспечение целостности и достоверности информации.

1.5. Обязанности и права ответственного за работу с СКЗИ определяются настоящей инструкцией положением и должностными регламентами, разрабатываемыми в соответствии с требованиями нормативных документов.

1.6. Ответственный за работу с СКЗИ в своей деятельности руководствуется законодательством Российской Федерации, нормативными актами, организационно-распорядительными документами «МБДОУ Детский сад №6 п.Смидович» и федеральных органов исполнительной власти, уполномоченных в области безопасности и защиты информации, с учетом требований настоящей инструкции, а также эксплуатационно-технической документации на СКЗИ.

2. Функции ответственного за работу с СКЗИ

2.1. Организация работ по подготовке объектов автоматизации «МБДОУ Детский сад № 6п.Смидович» к использованию СКЗИ, проверка их готовности, и участие в составлении заключений о допуске к самостоятельной работе со средствами СКЗИ.

2.2. Разработка мероприятий по обеспечению функционирования и безопасности, применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационно-технической документацией к этим средствам, в том числе с правилами пользования;

2.3. Организация обучения лиц, использующих СКЗИ, правилам работы с ними.

2.4. Поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним.

2.5. Учет обслуживаемых обладателей конфиденциальной информации, а также физических лиц, непосредственно допущенных к работе с СКЗИ.

2.6. Учет ключевой информации ключевых документов, их распределение.

2.7. Контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом и «Инструкцией 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» (регистрационный № 2848 от 06.08.2001 Минюста России).

2.8. Служебные проверки и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты информации ограниченного доступа, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

2.9. Организация эксплуатации автоматизированных рабочих мест с СКЗИ.

2.10. Оперативное решение всех вопросов, касающихся криптографической защиты информации.

2.11. Руководство деятельности персонала «МБДОУ Детский сад №6 п.Смидович» по соблюдению требований криптографической защиты информации, а также взаимодействие с лицензиатами, предоставляющими услуги в области шифрования информации.

3. Права, ответственность и обязанности ответственного за работу с СКЗИ

3.1. Ответственный за работу с СКЗИ имеют право:

3.1.1. Запрашивать и получать в пределах своей компетенции необходимые сведения и материалы для организации и проведения работ по вопросам обеспечения криптографической защиты информации.

3.1.2. Контролировать деятельность персонала «МБДОУ Детский сад №6 п.Смидович» по выполнению ими требований криптографической защиты информации.

3.1.3. Принимать участие в реализации организационно-технических мероприятий по криптографической защите информации.

3.1.4. Обеспечивать криптографическую защиту информации в соответствии с нормативными документами, а также осуществлять контроль и оценку эффективности принятых мер.

3.1.5. Вносить предложения руководству о принятии необходимых мер в случае обнаружения утечки или предпосылок к утечке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, и несанкционированного доступа к ней.

3.1.6. Участвовать в служебных проверках с целью выяснения причин выявленных нарушений установленных требований и норм в области обеспечения криптографической защиты информации.

3.1.7. Требовать, в необходимых случаях, от работников предоставления письменных объяснений по фактам установленных нарушений режима ограничения доступа и правил по криптографической защите информации.

3.2. На ответственного за работу с СКЗИ возлагается ответственность за:

3.2.1. Обеспечение установленного порядка криптографической защиты информации в «МБДОУ Детский сад №5 п.Смидович», в том числе порядка обращения с СКЗИ и криптоключами к ним.

3.2.2. Организацию выполнения работ по обеспечению криптографической защиты информации.

3.2.3. Выполнение требований нормативных документов в части криптографической защиты информации.

3.3. Ответственный за работу с СКЗИ обязан:

3.3.1. Соблюдать режим конфиденциальности при обращении со сведениями, которые ему доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых средств криптографической защиты информации.

3.3.2. Выполнять требования к обеспечению безопасности информации ограниченного доступа.

3.3.3. Надежно хранить СКЗИ, эксплуатационную и техническую документацию к ним.

3.3.4. Своевременно выявлять и фиксировать попытки посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документов к ним.

3.3.5. Немедленно принимать защитные меры по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов компрометации, утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

3.3.6. Вести поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов по установленным формам.

3.3.7. Изготовлять совместно с Лицензиатом из исходной ключевой информации ключевые документы, осуществлять их распределение, передачу и учет.

3.3.8. Проверять готовность работников «МБДОУ Детский сад №6 п.Смидович» к самостоятельному использованию СКЗИ и составлять заключения допуске к самостоятельной работе СКЗИ.

3.3.9. Обеспечивать функционирование и безопасность применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам.

3.3.10. Осуществлять контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, соответствующим сертификатом.

3.3.11. Проводить служебную проверку и составлять заключения по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты информации ограниченного доступа.

3.3.12. Разрабатывать и принимать меры по предотвращению возможных опасных последствий подобных нарушений.

3.3.13. Обучать лиц, использующих СКЗИ, правилам работы с ними.

3.3.14. Составлять и утверждать перечень пользователей СКЗИ с целью их допуска к работе с СКЗИ.

Приложение 3

УТВЕРЖДЕНО
приказом заведующего МБДОУ
«Детский сад № 6 п.Смидович»
Н.В. Филимонова
от 28.06.2024 г. № 38

ПОЛОЖЕНИЕ
по организации криптографической защиты информации

Термины и определения

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

Государственный контроль - проведение проверки выполнения юридическим лицом при осуществлении его деятельности обязательных требований, установленных федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

Доступ к информации - возможность получения информации и ее использования.

Закрытый ключ – криптографический ключ, который хранится абонентом в тайне. Он используется для формирования электронной подписи и шифрования.

Информация ограниченного доступа – информация, доступ к которой ограничен законодательством Российской Федерации или служебной необходимостью.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию.

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

Ключевой носитель — это машинный носитель информации для хранения закрытого ключа.

Компрометация ключевой информации – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность,

конфиденциальность, подтверждение авторства, невозможность отказа от авторства). Виды компрометации ключевой информации:

– **явная компрометация ключей** - компрометация, факт которой становится известным на отрезке установленного времени действия данного ключа;

неявная компрометация ключей - компрометация ключа, факт которой остается неизвестным для лиц, являющихся законными пользователями данного ключа.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Криптографическая защита информации – процесс преобразования исходной информации с целью ее защиты от несанкционированного доступа при помощи некоторого алгоритма, называемого шифром и использованеи электронной подписи.

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

МНИ – машинные носители информации.

Несанкционированный доступ к информации (НСД):

– получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

доступ к информации или ее носителям с нарушением правил доступа к ним.

Операционная система (ОС) - это специальный набор программ, благодаря которому все системы компьютера взаимодействуют как между собой, так и с пользователем.

Ответственный за работу с СКЗИ – ответственное должностное лицо, являющееся уполномоченным установленным порядком на проведение работ в области защиты криптографической информации. **Открытый ключ** - криптографический ключ, который связан с закрытым с помощью особого математического соотношения. Открытый ключ известен всем другим абонентам системы, он предназначен для проверки электронной подписи и позволяет определить автора подписи и достоверность электронного документа, но не позволяет вычислить закрытый ключ. Открытый ключ считается принадлежащим абоненту, если он был зарегистрирован (сертифицирован) установленным порядком.

ПО – программное обеспечение.

Пользователь – должностное лицо, допущенное в установленном порядке к самостоятельной работе с криптосредством, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

ПЭВМ (АРМ) – персональная электронно-вычислительная машина.

СКЗИ (Криптосредство) – шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Спецпомещения – помещения, в которых установлены криптосредства или хранятся ключевые документы к ним.

Средство защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Средства имитозащиты - аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

Средства электронной подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи, создание закрытых и открытых ключей электронной подписи.

1. Общие положения

Положение по организации криптографической защиты информации (далее – Положение) разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом от 06.04.2011 N 63-ФЗ "Об электронной подписи", Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66, Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России, № 149/6/6-622, 2008 г., далее - Типовые требования ФСБ России), Приказа ФСБ России от 10 июля 2014 г. № 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».

1.1. Положение определяет в «МБДОУ Детский сад №6 п.Смидович» единый порядок:

- организации и обеспечения безопасности функционирования шифровальных (криптографических) средств (далее – криптосредства);
- эксплуатации криптосредств;
- организации и обеспечения безопасности хранения, обработки и передачи по каналам связи информации, не содержащей сведений, составляющих государственную тайну, подлежащей защите с использованием криптосредств.

1.2. Инструкция является нормативным документом обязательным для выполнения (в части касающейся) всеми работниками «МБДОУ Детский сад № 6 п.Смидович»

1.3. Криптосредства с введенными ключами и МНИ с записанной на них (исходной) ключевой информацией относятся к материальным носителям,

содержащим информацию ограниченного доступа. При этом должны выполняться требования настоящей Инструкции и иных документов, регламентирующих порядок обращения в «МБДОУ Детский сад №6 п.Смидович» с информацией ограниченного доступа и ее носителями.

2. Организация и обеспечение безопасности обработки с использованием шифровальных (криптографических) средств защищаемой информации

2.1. Безопасность обработки защищаемой информации с использованием криптосредств организует и обеспечивает ответственный за работу с СКЗИ.

2.2. Ответственный за работу с СКЗИ несет ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи защищаемой информации с использованием криптосредств требованиям действующего законодательства и нормативных документов ФСБ России (включая Типовые требования ФСБ России) и ФСТЭК России, лицензионным требованиям и условиям, правилам пользования криптосредствами, эксплуатационной и технической документации к криптосредствам, а также требованиям настоящей Инструкции.

2.3. Организация и обеспечение эксплуатации криптосредств, а также разработка и осуществление мероприятий по обеспечению безопасности сбора, ввода, хранения, использования и передачи защищаемой информации с применением криптосредств в «МБДОУ Детский сад №6 п.Смидович» возлагается на ответственного за работу с СКЗИ.

2.4. Работа ответственного за работу с СКЗИ по организации криптографической защиты проводится на плановой основе.

2.5. Задачи ответственного за работу с СКЗИ:

- ведение поэкземплярного учета криптосредств, технической и эксплуатационной документации к ним, правил работы с криптосредствами и ключевых документов, имеющихся в «МБДОУ Детский сад №6 п.Смидович»;
- обеспечение соблюдения принципа персональной ответственности пользователей криптосредств и владельцев ключей шифрования и ЭП за сохранность криптосредств и ключей шифрования;
- учет пользователей криптосредств;
- принятие участия в установке и ввод в эксплуатацию криптосредств;
- обучение пользователей, с оформлением соответствующего заключения и внесения данных об обучении в журнал учёта обучения пользователей СКЗИ;
- контроль за наличием криптосредств, технической и

эксплуатационной документации к ним, правил пользования криптосредств и ключевых документов, а также за соблюдением пользователями криптосредств и владельцами ключей шифрования и ЭП правил обращения с ними;

- организация и осуществление приема-передачи криптосредств в случае смены пользователей;
- участие в уничтожении ключевой информации с пользователями криптосредств и (или) владельцами ключей шифрования и ЭП, а также в деинсталляции программного обеспечения криптосредств из АРМ пользователей с составлением соответствующих актов;

2.17. Пользователям криптосредств запрещается:

- разглашать закрытую ключевую информацию и другую информацию ограниченного доступа, передавать без разрешения ответственного за работу с СКЗИ другим лицам криптосредства, носители ключевой информации и пароли, выводить закрытую ключевую информацию на монитор и принтер;
- вносить какие-либо несанкционированные изменения в криптосредство и в аппаратно-программные средства, работающие совместно с установленным криптосредством и способными влиять на функционирование криптосредства;
- изменять настройки криптосредств;
- осуществлять вскрытие системных блоков ЭВМ с установленными криптосредствами, подключать к ним дополнительные устройства без разрешения ответственного за работу с СКЗИ;
- оставлять без контроля ключевые носители, а также ЭВМ с установленными криптосредствами при включенном питании;
- выводить на монитор информацию ограниченного доступа, обрабатываемую с использованием криптосредств в присутствии лиц, не имеющих к этой информации непосредственного отношения;
- выносить ключевые носители за пределы служебных помещений без разрешения руководителя структурного подразделения «МБДОУ Детский сад №6 п.Смидович» и\или ответственного за работу с СКЗИ;
- применять скомпрометированные ключи или пароли;
- осуществлять несанкционированное копирование ключевой информации;
- вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным порядком использования ключевого носителя;
- производить записи новых ключей на машинные носители ключевой информации без предварительного уничтожения ранее записанной ключевой информации, если иной порядок не определен эксплуатационной

документацией.

В случае обнаружения факта несанкционированного доступа к системным блокам, наличия «посторонних» (незарегистрированных) программ, нарушения целостности программного обеспечения работа на этих технических средствах должна быть прекращена. По данному факту комиссией «МБДОУ Детский сад №5 п.Смидович» проводится служебная проверка и организуются работы по анализу и ликвидации негативных последствий нарушения.

Владельцы ключей шифрования и ЭП несут полную ответственность за обеспечение сохранности, неразглашения и нераспространения ключей и ключевой информации.

3. Порядок обращения с криптосредствами и криптоключами к ним. Мероприятия при компрометации криптоключей

3.1. В «МБДОУ Детский сад №6 п.Смидович» для организации и обеспечения безопасности хранения, обработки и передачи по каналам связи защищаемой информации используются криптосредства, реализующие шифрование информации в телекоммуникационных сетях и криптосредства реализующие функции удостоверения электронных документов электронной подписью.

Криптографические ключи применяемых криптосредств, в зависимости от требований правил пользования, записываются и хранятся на МНИ и/или на электронных ключевых носителях многократного (долговременного) использования (Flash-накопители, Data Key, Smart Card, Touch Memory, eToken и т.д.).

3.2. Передача по техническим средствам связи служебных сообщений, касающихся организации и обеспечения безопасности с использованием криптосредств защищаемой информации, производится только в зашифрованном виде.

Передача по техническим средствам связи закрытых ключей не допускается, за исключением специально организованных систем, правилами пользования которыми предусматривается управление ключевой системой с использованием технических каналов связи.

3.3. Криптосредства, эксплуатационная и техническая документация, правила пользования и ключевые документы между пользователями не передаются.

На период отсутствия основного пользователя по приказу руководителя «МБДОУ Детский сад №6 п.Смидович» может быть произведена временная передача криптосредств, для обеспечения непрерывности технологического процесса обмена информацией. Ключевые документы при этом передавать

категорически запрещается.

Указанная передача осуществляется только через ответственного за работу с СКЗИ.

3.4. Передача криптосредств, эксплуатационных, технических документов к ним, правил пользования и ключевой документации между «МБДОУ Детский сад №6 п.Смидович» и иными организациями (за исключением случаев, когда это предусмотрено заключенными с ними Соглашениями об обмене электронными документами с использованием средств криптозащиты) осуществляется с разрешения (уведомления) ответственного за работу с СКЗИ.

3.5. Аппаратные компоненты криптосредства, а также аппаратные средства, с которыми осуществляется штатное функционирование криптосредства должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) криптосредства, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

3.6. При необходимости работы с одного рабочего места нескольких пользователей каждому пользователю криптосредства должен вырабатываться и выдаваться в установленном порядке индивидуальный набор ключевых документов и паролей.

3.7. Ответственным за работу с СКЗИ ведется поэкземплярный учет криптосредств[1], эксплуатационной и технической документации к ним, правил пользования[2], ключевых документов, а также осуществляется контроль за их движением с момента поступления (инсталляции) и до уничтожения (деинсталляции, возврата). Основным принципом учета является одноразовость регистрации[3].

3.8. Основным требованием при организации учета криптосредств, эксплуатационной и технической документации к ним, правил пользования, а также ключевых документов является создание системы регистрации, позволяющей обеспечить персональную ответственность работников «МБДОУ Детский сад №5 п.Смидович» за их сохранность.

3.9. Передача криптосредств, технической и эксплуатационной документации к ним, правил пользования, ключевых документов пользователям «МБДОУ Детский сад №6 п.Смидович», непосредственно

---

[1] Учет криптосредств, которые не имеют собственных уникальных номеров, производится по номерам технических средств, в которые они встраиваются.

[2] Учет и выдача под роспись в журнале технической, эксплуатационной документации и правил пользования производится в случае, если они имеют свои уникальные регистрационные номера и поступают или размножены в виде отдельных документов.

[3] Под регистрацией понимается оформление факта получения или создания документа в установленных формах учета.

отвечающим за дальнейшую работу с ними (обработку, хранение, дальнейшую пересылку, установку, уничтожение и т. д.) производится под роспись в журналах учета или в необходимых случаях по акту с отметкой о номере акта в соответствующем журнале учета.

3.10. Ответственным за работу с СКЗИ ведется Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, правил пользования и ключевых документов, являющийся журналом основного учета по форме.

В данном журнале должны быть зарегистрированы все криптосредства, документация и ключевые документы к ним, используемые при организации и осуществлении криптографической защиты в «МБДОУ Детский сад №6 п.Смидович», в т.ч. находящиеся на хранении, предназначенные для пересылки, полученные во временное пользование и т.п.

Учитывать в Журнале поэкземплярного учета криптосредств другие средства защиты, не являющиеся криптосредствами, не допускается.

3.11. При наличии возможности маркировка МНИ осуществляется простановкой регистрационного штампа и нанесением следующих реквизитов: учетного номера, ФИО пользователя криптосредства.

При отсутствии возможности (из-за размеров) нанесения всех учетных данных на МНИ (Touch Memory, eToken, флэш-носители и.п.) разрешается прикреплять специально изготовленные бирки с нанесенными учетными данными.

3.12. Отметки об уничтожении записанной на МНИ информации производятся в формах учета, где была зарегистрирована указанная выше информация.

3.13. Если правилами пользования криптоключи вводят и хранят (на весь срок их действия) непосредственно в криптосредстве, то такая электронная запись криптоключа должна регистрироваться в аппаратном журнале учета эксплуатации криптосредств.

3.14. При ведении журналов учета применение подчисток, использование корректирующих средств и т.п. не допускается.

При необходимости исправления произведенной записи текст, подлежащий исправлению, аккуратно зачеркивается без сокрытия его содержания, и на свободном месте Журнала производится запись: «испр. верить». Запись заверяется подписью лица, ответственного за ведение Журнала.

3.15. Журналы поэкземплярного учета ведутся до полного использования, после чего закрываются в установленном порядке.

Все числящиеся за «МБДОУ Детский сад №6 п.Смидович» на момент окончания журнала криптосредства, эксплуатационная и техническая

документация к ним, правила пользования, ключевые документы берутся на учет во вновь заведенном журнале поэкземплярного учета лицом, ответственным за ведение журнала.

3.16. Допускается учет криптосредств, эксплуатационной и технической документации, правил пользования и ключевых документов вести в электронном виде.

При этом учет должен отвечать следующим требованиям:

- наличие в системе автоматически формируемого протокола изменений учетных данных (недоступного для корректировки лицом, ответственным за учет);
- гарантированное обеспечение сохранности учетных данных (проведение ежедневного резервного копирования);
- возможность их документирования на бумажных носителях и отчуждаемых МНИ.

В случае отсутствия таких программных средств ведение электронного журнала должно предусматривать возможность проверки каждой его записи подтверждающим документом на бумажном носителе, т.е. наличие сопроводительных писем о поступлении криптосредств, доверенности на получение ключевой информации, акта изготовления ключевого носителя, подписанных пользователем и ответственным за работу с СКЗИ распечатки открытых ключей и т.д.

Закрытие электронного журнала производится порядком, аналогичным описанному в п. 3.16, после чего осуществляется запись учетных данных, подписанных ЭП ответственного за учет на CD\DVD диск.

3.17. При увольнении, переводе на другую работу ответственного за работу с СКЗИ, ведущего учет криптосредств, техническая, эксплуатационная документация к ним, правила пользования, ключевые носители и документов, дистрибутивы (копии дистрибутивов) криптосредства, техническая, эксплуатационная документация к ним, правила пользования, ключевые носители и документы передаются вновь назначенному работнику по акту.

Криптосредства, ключевые документы, правила пользования, эксплуатационная и техническая документация могут доставляться фельдъегерской связью или специально выделенными нарочными из числа работников «МБДОУ Детский сад №6 п.Смидович» (по доверенности), при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки. Возможна передача правил пользования по техническим каналам связи в зашифрованном виде.

3.18. При пересылке программного обеспечения криптосредств ключевые носители и документы должны быть помещены в прочную упаковку,

исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

Оформленную таким образом упаковку, при предъявлении фельдсвязью дополнительных требований, помещают во внешнюю упаковку, оформленную согласно предъявляемым требованиям.

3.19. Пересылка криптосредств, правил работы, ключевых носителей и документов осуществляется с сопроводительным письмом, в котором необходимо указать, что посылается и в каком количестве, учетные номера, экземпляры документов, а также назначение и порядок использования высылаемого приложения. В случае если приложение направляется адресату в нескольких упаковках, сопроводительное письмо вкладывают в одну из упаковок. На упаковках проставляется пометка «Лично». Криптосредства пересылаются отдельно от ключевых документов к ним.

Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает отправителю, а при необходимости информирует об этом ответственного за работу с СКЗИ и орган почтовой связи. В этом случае поступившие ключевые документы до получения указаний от отправителя и ответственного за работу с СКЗИ применять не разрешается.

3.20. Получение криптосредств, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме.

Отправитель обязан контролировать доставку своих отправлений адресатам.

Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

3.21. Криптосредства уничтожаются по указанию ответственного за работу с СКЗИ в установленные им сроки. Вместе с выводимыми из эксплуатации криптосредствами подлежат уничтожению техническая и эксплуатационная документация к ним и правила пользования.

Уничтожение программных криптосредств, инсталлированных на аппаратные средства, производится по согласованию с ответственным за работу с СКЗИ.

3.22. Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они записаны, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (Flash-накопителей, Data Key, Smart Card, Touch Memory, eToken и т.п.).

Удаление информации с магнитных носителей может осуществляться с использованием систем гарантированного уничтожения информации.

Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим типам криптосредств.

Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожаются путем сжигания или перерабатываются с помощью бумагорезательных машин.

3.23. Предназначенные к уничтожению (утилизации) криптосредства подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом криптосредства считаются изъятыми (деинсталлированными) из аппаратных средств, если выполнены предусмотренные эксплуатационной и технической документацией к криптосредствам процедуры удаления. Деинсталлирование программного обеспечения криптосредств производится ответственным за работу с СКЗИ с занесением соответствующих отметок в журналы учета.

3.24. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному за работу с СКЗИ или по его указанию должны быть уничтожены в установленном порядке на месте.

Ключевые документы должны быть уничтожены или возвращены в орган криптографической защиты в сроки, указанные в правилах пользования к соответствующим типам криптосредств, но не позднее 10 суток с момента окончания срока их действия (вывода из действия). Отметки о деинсталляции криптосредств, уничтожении эксплуатационной, технической документации, правил пользования, ключевых документов оформляются в соответствующих журналах учета.

3.25. В «МБДОУ Детский сад №6 п.Смидович» ключевые документы и

носители ключевой информации уничтожаются под роспись в соответствующих журналах поэкземплярного учета.

По решению ответственного за работу с СКЗИ ключевые документы могут быть уничтожены на месте пользователями криптосредства или владельцами ключей шифрования и ЭП совместно с ответственным за работу с СКЗИ под расписку в соответствующих журналах учета. При этом, пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи.

3.26. Уничтожение по акту производится комиссией в составе не менее двух человек. В состав комиссии в обязательном порядке включается ответственный за работу с СКЗИ. В акте указывается, что уничтожается и в каком количестве, серии, учетные номера, экземпляры. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров, уничтожаемых криптосредств, правил пользования, эксплуатационной и технической документации, ключевых документов.

Исправления в тексте акта не допускаются. В случае обнаружения комиссией неточностей в тексте акта в процессе уничтожения, они должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах учета. Акт утверждается руководителем «МБДОУ Детский сад №6 п.Смидович».

3.27. В случаях недостачи, не предъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску. О данном факте незамедлительно информируется ответственный за работу с СКЗИ, от которого были получены ключевые документы. Если в течение суток с момента выявленного факта недостачи предпринятые меры поиска не дали положительных результатов, руководителем «МБДОУ Детский сад №5 п.Смидович» назначается проведение служебной проверки с участием ответственного за работу с СКЗИ и работников других структурных подразделений «НАИМЕНОВАНИЕ УЧРЕЖДЕНИЯ» «МБДОУ Детский сад №6 п.Смидович» с составлением акта.

3.28. О нарушениях, которые могут привести к компрометации криптоключей или передававшейся (хранящейся) с их использованием информации, пользователи криптосредств, владельцы ключей шифрования и ЭП обязаны сообщать ответственному за работу с СКЗИ, от которого были получены ключевые документы.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их

копирования (чтения, размножения).

3.29. События, квалифицируемые как явная компрометация ключей:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение работников, имевших доступ к ключевой информации;
- нарушение печати на сейфе, пенале с ключевыми носителями;
- нарушение правил хранения и уничтожения (после окончания срока действия) ключевой информации;
- наличие подписи под входящим документом сертификата, находящегося в списке отозванных сертификатов;
- 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);

3.30. К событиям, квалифицируемым как подозрение о наличии факта компрометации криптографического ключа, требующим проведения проверки и принятия решения на предмет происшествия явной компрометации, относится возникновение подозрений в утечке информации в системе защищенной связи.

3.31. Основные правила в принятии решения о компрометации:

- в случае признания факта компрометации любого из закрытых ключей, записанных на ключевом носителе абонента, признаются непосредственно скомпрометированными все ключи на данном носителе. Данный абонент признается непосредственно скомпрометированным;
- в случае признания факта непосредственной компрометации любого из ключей у любого абонента коллектива[4] однозначно признаются скомпрометированными все ключи, общие для абонентов данного коллектива. Пользователи коллектива, не подвергшиеся непосредственной компрометации, признаются косвенно скомпрометированными. У пользователей коллектива, не подвергшихся непосредственной компрометации, не скомпрометированными могут быть признаны только индивидуальные ключи (персональный ключ, закрытый ключ ЭП);
- в случае признания факта компрометации любого из закрытых ключей, записанных на жестком диске, признаются скомпрометированными все ключи данного АРМа;
- в случае компрометации ключей хотя бы одного администратора ключевого центра считается скомпрометированной вся ключевая информация в

[4] Совокупность абонентов одного сетевого узла, имеющих одинаковые ключи для шифрования информации (используется при описании ПО ViPNet).

сети.

3.32. При наступлении любого из перечисленных в п. 3.30 событий или подозрении в компрометации ключа пользователь криптосредства должен немедленно прекратить связь с другими пользователями и сообщить о факте компрометации (или предполагаемом факте компрометации) ответственному за работу с СКЗИ.

По факту компрометации ключей должна быть проведена служебная проверка. Выведенные из действия скомпрометированные ключи после проведения служебной проверки подлежат уничтожению порядком, определенным настоящим Ппложением.

3.33. На замену скомпрометированных ключей пользователю криптосредства, владельцу ключей шифрования и ЭП ответственным за работу с СКЗИ выдаются новые ключи.

В отношении ключей, по поводу которых возникло подозрение в их компрометации, проводится проверка комиссией. Возможность дальнейшего использования указанных ключей определяется в соответствии с выводами комиссии.

3.34. Порядок действия пользователей и администраторов удостоверяющих центров при компрометации ключей определяется Регламентом работы удостоверяющего центра.

4. Эксплуатация криптосредств и обеспечение безопасности информации при передаче по каналам связи

4.1. При использовании ЭВМ с установленными криптосредствами, подключенных к информационно-телекоммуникационным сетям общего пользования, с целью исключения возможности несанкционированного доступа к среде функционирования криптосредств, компонентам криптосредств, а также к системным ресурсам используемых операционных систем со стороны указанных сетей должны выполняться требования Указа Президента Российской Федерации от 17 марта 2008 г. «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» и требования, определенные в соответствии с принятой в «МБДОУ Детский сад №6 п.Смидович» политикой безопасности (установка межсетевых экранов, средств обнаружения вторжений, организация VPN сетей и т.п.).

4.2. Для обеспечения деятельности «МБДОУ Детский сад №6 п.Смидович» по обмену различной информацией при решении возложенных на них задач используется информационная телекоммуникационная корпоративная сеть передачи данных (далее – КСПД). Эта сеть является

транспортной инфраструктурой передачи данных. Для целей обеспечения безопасности передаваемой защищаемой информации указанная сеть должна эксплуатироваться в защищенном варианте с использованием криптосредств.

4.3. Принципы организации сетевой защиты, технологические решения построения, использование криптосредств, порядок подключения иных организаций, организация доступа пользователей, требования по размещению, установке и эксплуатации технических средств определяются отдельным документом по организации сетевой защиты информации в КСПД.

4.4. Перед установкой криптосредств необходимо проверить программное обеспечение ЭВМ на отсутствие вирусов.

4.5. На ЭВМ не должны устанавливаться средства разработки программного обеспечения и программы-отладчики. Если наличие средства отладки приложений обусловлено технологическими потребностями, то его использование должно быть санкционировано ответственным за работу с СКЗИ.

4.6. Для обеспечения защиты от несанкционированного доступа (НСД) «МБДОУ Детский сад №6 п.Смидович», используются электронные ключи и\или система парольной защиты.

5. Особенности организации защиты информации и применения криптосредств в случае их использования для обеспечения безопасности персональных данных

5.1. Работа по обеспечению безопасности персональных данных, обрабатываемых в информационных системах «МБДОУ Детский сад №6 п.Смидович» проводится в рамках обеспечения безопасности информации «МБДОУ Детский сад № 6 п.Смидович» в целом и должна отвечать общим требованиям, изложенным в 1-4 разделах настоящей Инструкции.

Особенности организации защиты персональных данных обусловлена телекоммуникационной средой передачи данных.

5.2. Обмен в электронной форме защищаемой информацией с иными организациями допускается только с использованием сертифицированных в системе сертификации ФСБ России шифровальных (криптографических) средств. При этом класс шифровальных (криптографических) средств, используемых иными организациями, должен быть не ниже класса шифровальных (криптографических) средств, используемых в «МБДОУ Детский сад №6 п.Смидович» для обмена информацией с этой внешней организацией.

5.3. Все передаваемые персональные данные граждан в открытом виде могут быть представлены только на определенных рабочих местах работников «МБДОУ Детский сад №6 п.Смидович». Сведения граждан должны быть

защищены и недоступны для третьих лиц. Программно-аппаратные средства иных организаций, используемые при информационном обмене не должны снимать ЭП и переподписывать другой ЭП защищаемую информацию.

5.4. Взаимодействие программно-аппаратных средств операторов связи с КСПД должно осуществляться только через сертифицированные средства межсетевой защиты.

6. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним

6.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее – спецпомещения), должны обеспечивать сохранность информации ограниченного доступа, криптосредств и ключевых документов.

6.2. Перечисленные в настоящей Инструкции требования к спецпомещениям могут не предъявляться, если это предусмотрено правилами пользования криптосредствами, согласованными с ФСБ России.

6.3. При оборудовании спецпомещений должны выполняться требования к размещению и установке криптосредств, а также других средств, совместно функционирующих с криптосредствами, предусмотренных правилами пользования.

6.4. Помещения, в которых размещены криптосредства (помещения с рабочими местами пользователей криптосредств, серверных помещений «МБДОУ Детский сад №6 п.Смидович», ответственного за работу с СКЗИ должны иметь прочные входные двери с замками, гарантирующими надежное закрытие дверей в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно несанкционированное проникновение в помещения посторонних лиц, должны быть оборудованы охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

6.5. Работоспособность охранной сигнализации проверяется ответственным лицом при сдаче помещения под охрану.

6.6. Размещение, оборудование, охрана и организация режима работы в спецпомещении ответственному за работу с СКЗИ должны **исключить** возможность неконтролируемого проникновения или бесконтрольного пребывания в них посторонних лиц, а также просмотра посторонними лицами информации ограниченного доступа.

6.7. Режим охраны и порядок доступа работников и посетителей, уборка

спецпомещений, контроль за состоянием технических средств охраны определяется отдельной инструкцией.

6.8. Двери спецпомещения ответственного за работу с СКЗИ (в его отсутствии) и серверных (в любое время) должны быть закрыты на замок и могут открываться только для санкционированного прохода определенного перечня работников. Ключи от замков входных дверей нумеруют, учитывают в журнале учета хранилищ и выдаются ответственному за работу с СКЗИ под роспись. Дубликаты ключей от замков входных дверей спецпомещений подлежат хранению в сейфе руководителя структурного подразделения или руководителя «МБДОУ Детский сад №6 п.Смидович».

6.9. Для предотвращения просмотра извне окна спецпомещений ответственного за работу с СКЗИ и серверных помещений должны быть защищены (шторы, жалюзи, светоотражающая пленка и т.д.).

6.10. Ответственный за работу с СКЗИ для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей, должен иметь необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и приспособлениями для опечатывания.

Опечатанные дубликаты ключей от хранилищ, должны быть сданы под расписку в журнале сдачи и выдачи ключей от хранилищ руководителю структурного подразделения. По окончании рабочего дня спецпомещения должны быть закрыты на замки и сданы на пост охраны в рамках системы контроля доступа.

Ключи от спецпомещений в опечатанном тубусе должны быть сданы под расписку в соответствующем журнале дежурному службы охраны одновременно с передачей под охрану самих помещений. В случае сдачи помещений вневедомственной охране (на пульт централизованного наблюдения) тубусы сдаются под расписку руководителю структурного подразделения.

Средства, предназначенные для опечатывания хранилищ, должны находиться у работников, ответственных за эти хранилища.

6.11. При утрате ключа от хранилища или от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с оформлением акта.

6.12. Спец помещения и находящиеся в них опечатанные хранилища могут быть вскрыты только ответственными работниками или в экстренных случаях, в их отсутствие, специально назначенной комиссией по указанию руководителя «МБДОУ Детский сад №6 п.Смидович».

6.13. При обнаружении признаков, указывающих на возможное

несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководителю структурного подразделения и ответственному за работу с СКЗИ. Ответственный за работу с СКЗИ должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий и замене скомпрометированных криптоключей.

6.14. Размещение криптосредств, а также другого оборудования, функционирующего с криптосредствами, в спецпомещениях пользователей криптосредств должны **свести к минимуму** возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей должны осуществляться в отсутствие лиц, не допущенных к работе с данными криптосредствами.

6.15. На время длительного отсутствия пользователей криптосредства их рабочие станции должны быть выключены. При необходимости, по согласованию с ответственным за работу с СКЗИ, рабочие станции на период отсутствия пользователей криптосредств могут быть использованы вновь назначенными пользователями криптосредств со своими индивидуальными ключами.

6.16. В спецпомещениях пользователей криптосредств и владельцев ключей шифрования и ЭП для хранения выданных им ключевых документов необходимо иметь запираемые шкафы (ящики, хранилища) индивидуального пользования.

6.17. Один ключ от хранилища должен находиться у пользователя криптосредства или владельца ключей шифрования и ЭП. Дубликаты ключей от хранилищ, опечатанные личными печатями указанных лиц, сдаются на хранение под роспись в соответствующем журнале руководителю структурного подразделения. В случае отсутствия хранилищ у пользователей криптосредств и владельцев ключей шифрования и ЭП по окончании рабочего дня ключевые документы в опечатанных тубусах (пеналах, коробках), сдаются на хранение руководителю структурного подразделения или ответственному за работу с СКЗИ.

6.18. При утрате ключа от замков хранилищ или от входной двери в помещение пользователя криптосредства замок или секрет замка необходимо заменить.

6.19. Опечатанные хранилища пользователей криптосредств могут быть вскрыты только самими пользователями. В исключительных случаях разрешается вскрытие специально назначенной комиссией с разрешения руководителя «МБДОУ Детский сад №5 п.Смидович».

7. Контроль за организацией и обеспечением безопасности защищаемой информации

7.1. Контроль за соблюдением правил пользования и условий их использования, указанных в правилах пользования, осуществляется ответственным за работу с СКЗИ во всех структурных подразделениях «МБДОУ Детский сад №6 п.Смидович».

ФСБ России осуществляет государственный контроль.

7.2. Государственный контроль за выполнением требований к обеспечению безопасности использования криптосредств, применяемых в информационных системах персональных данных, осуществляется в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» без ознакомления с персональными данными.

7.3. Непосредственный допуск к проверке комиссии ФСБ России или уполномоченных представителей федеральных (территориальных) органов ФСБ России осуществляет руководитель «МБДОУ Детский сад №6 п.Смидович», при предъявлении удостоверения (предписания) на право проверки, заверенного печатью, и документов, удостоверяющих личность.

7.4. Удостоверения (предписания) на право проверки подписывают Руководитель ФСБ России, его заместители, а также по их указанию – руководители федеральных (территориальных органов ФСБ России). Допуск к проверке возможен на основании указаний этих лиц, переданных по техническим каналам связи.

7.5. Ответственный за работу с СКЗИ допускается к проверке в соответствии с указаниями руководителя«МБДОУ Детский сад №6 п.Смидович» .

7.6. По результатам контроля составляется акт (справка). С актом проверки (справкой) под расписку должен быть ознакомлен руководитель«МБДОУ Детский сад №6 п.Смидович» и ответственный за работу с СКЗИ.

7.7. Руководитель«МБДОУ Детский сад №6 п.Смидович» , структурных подразделений «МБДОУ Детский сад №6 п.Смидович», ответственный за работу с СКЗИ обязаны принять безотлагательные меры к устранению вскрытых проверкой недостатков и выполнению рекомендаций, изложенных в акте (справке) проверки. Сообщения о принятых мерах должны быть представлены в установленные проверяющими сроки.

8. Ответственность за нарушение безопасности информации в «МБДОУ Детский сад №5 п.Смидович»**.**

8.1. Лица, виновные в нарушении правил пользования криптосредствами, могут быть привлечены к административной или

дисциплинарной ответственности.

8.2. Лица, виновные в нарушении безопасности информации информационных системах «МБДОУ Детский сад №6 п.Смидович», несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 4

УТВЕРЖДЕНА
приказом заведующего МБДОУ
Детский сад № 6 п.Смидович»
Н.В. Филимонова
от 28.06.2024 г. № 38

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00E719B594F57DA57381EAD5AC67BBA67C
Владелец: Филимонова Наталья Вадимировна
Действителен: с 08.09.2023 до 01.12.2024

ИНСТРУКЦИЯ
пользователю СКЗИ

Обеспечение безопасности применения криптосредств в «МБДОУ Детский сад №6 п.Смидович» организовано и проводится в соответствии с «инструкцией по организации криптографической защиты информации в «МБДОУ Детский сад №6 п.Смидович».

Обязанности пользователей криптосредств – работников «МБДОУ Детский сад №6 п.Смидович»**:**

- сохранять конфиденциальность информации, которая стала известной в процессе выполнения должностных обязанностей, в том числе сведений о закрытых криптографических ключах, паролях и применяемых криптосредствах, организации хранения, обработки и передачи по каналам связи информации с использованием криптосредств;
- хранить ключевую информацию, эксплуатационную документацию к криптосредствам на бумажных и машинных носителях в шкафах (ящиках, хранилищах) индивидуального пользования, в условиях, исключающих бесконтрольный доступ к ним, а также их искажение или несанкционированное уничтожение;
- во внерабочее время ключевые носители с криптоключами хранить в запираемом на замок и опечатанном индивидуальном хранилище или сдавать на хранение ответственному за работу с СКЗИ;
- выполнять требования эксплуатационных и регламентирующих документов по обеспечению безопасности защищаемой информации, обрабатываемой с применением криптосредств;
- сообщать руководителю «МБДОУ Детский сад №6 п.Смидович» и ответственному за работу с СКЗИ о ставших ему известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;
- немедленно сообщать своему руководителю с последующим уведомлением ответственного за работу с СКЗИ о фактах утраты криптосредств, эксплуатационной документации и ключевых документов к ним, ключей от помещений, хранилищ, личных номерных печатей,

нарушении печатей (наклеек), которыми опечатан системный блок ЭВМ с установленным криптосредством, компрометации ключевой информации и о других фактах, которые могут привести к разглашению защищаемой информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;

- в случае временного отсутствия (болезнь, командировка, отпуск и т.д.) ключевые носители и пароль оставить на хранение в сейфе начальника структурного подразделения (начальника отдела);
- при передаче ЭВМ с установленным криптосредством в ремонт (на замену, уничтожение), при переустановке программного обеспечения и т.д. сдавать эксплуатационную документацию к криптосредствам, ключевые носители и документы ответственному за работу с СКЗИ. При этом работником органа криптографической защиты информации в ЭВМ должно быть деинсталлировано программное обеспечение криптосредств с сохранением архивов на учтенном машинном носителе и с оформлением акта (под роспись в журнале учета) на уничтожение криптосредств;
- при увольнении, переводе на работу, не связанную с использованием криптосредств (изменении функциональных обязанностей, не предусматривающих необходимость использования криптосредств), эксплуатационную документацию к криптосредствам, а также ключевые носители сдать с документальным оформлением (под роспись) ответственному за работу с СКЗИ.

Пользователям криптосредств запрещается:

- разглашать закрытую ключевую информацию и другую информацию ограниченного доступа, передавать криптосредства, носители ключевой информации и пароли без разрешения ответственного за работу с СКЗИ и без расписки другим лицам, выводить закрытую ключевую информацию на монитор и принтер;
- вносить какие-либо несанкционированные изменения в криптосредство и в аппаратно-программные средства, работающие совместно с установленным криптосредством и способными влиять на функционирование криптосредства;
- изменять настройки криптосредств;
- осуществлять вскрытие системных блоков ЭВМ с установленными криптосредствами, подключать к ним дополнительные устройства без разрешения ответственного за работу с СКЗИ;
- оставлять без контроля ключевые носители, а также ЭВМ с установленными криптосредствами при включенном питании;
- выводить на монитор информацию ограниченного доступа, обрабатываемую с использованием криптосредств в присутствии лиц, не имеющих к этой информации непосредственного отношения;

- выносить ключевые носители за пределы служебных помещений без разрешения начальника структурного подразделения, руководителя «МБДОУ Детский сад №6 п.Смидович», ответственного за работу с СКЗИ;
- применять скомпрометированные ключи или пароли;
- осуществлять несанкционированное копирование ключевой информации;
- вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным порядком использования ключевого носителя;
- производить записи новых ключей на машинные носители ключевой информации без предварительного уничтожения ранее записанной ключевой информации, если иной порядок не определен эксплуатационной документацией.

Передача и хранение криптосредств.

Криптосредства, эксплуатационная и техническая документация, правила пользования и ключевые документы между пользователями не передаются.

На период отсутствия основного пользователя по приказу руководителя «МБДОУ Детский сад №6 п.Смидович» может быть произведена временная передача криптосредств, для обеспечения непрерывности технологического процесса обмена информацией. **Ключевые документы при этом передавать категорически запрещается.**

Указанная передача осуществляется только через ответственного за работу с СКЗИ.

Хранение ключевых документов пользователями криптосредств должно осуществляться в металлических шкафах (сейфах, отдельных ячейках сейфов) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним.

О нарушениях, которые могут привести к компрометации криптоключей или передававшейся (хранящейся) с их использованием информации, пользователи криптосредств, владельцы ключей шифрования и ЭП обязаны сообщать ответственному за работу с СКЗИ, от которого были получены ключевые документы.

События, квалифицируемые как явная компрометация ключей:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение работников, имевших доступ к ключевой информации;
- нарушение печати на сейфе с ключевыми носителями;
- нарушение правил хранения и уничтожения (после окончания срока действия) ключевой информации;
- наличие подписи под входящим документом сертификата, находящегося в списке отозванных сертификатов;

- 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);

К событиям, квалифицируемым как подозрение о наличии факта компрометации криптографического ключа, требующим проведения служебной проверки и принятия решения на предмет происшествия явной компрометации, относится возникновение подозрений в утечке информации в системе защищенной связи.

Ответственность за нарушение безопасности информации ИС «МБДОУ Детский сад №6 п.Смидович» **«НАИМЕНОВАНИЕ УЧРЕЖДЕНИЯ».**

Лица, виновные в нарушении правил пользования криптосредствами, могут быть привлечены к административной или дисциплинарной ответственности.

Лица, виновные в нарушении безопасности информации ИС «МБДОУ Детский сад №6 п.Смидович» , несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 5

ВЕРЖДЕНА
казом заведующего МБДОУ
тский сад № 6 п.Смидович»
Н.В. Филимонова
от 28.06.2024 г. № 38

ПОЛИТИКА

назначения и смены паролей для автоматизированных рабочих мест с установленными СКЗИ

Настоящая политика разработана в соответствии с требованиями эксплуатационной документации на средства криптографической защиты информации и применяется для назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.) для автоматизированных рабочих мест с установленными средствами криптографической защиты информации:

1. Для паролей на вход в ОС используются глобальная доменная «Политика паролей». Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.

2. Для паролей на вход в BIOS необходимо использовать фильтры паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п .);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;

- личный пароль пользователь не имеет права сообщать никому;

- смена паролей производиться не реже одного раза в 6 месяцев.

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

3. Шифрование на пароле в «МБДОУ Детский сад №6 п.Смидович» не применяется.

Приложение 6

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

УТВЕРЖДЕНА
приказом заведующего МБДОУ
«Детский сад № 6 п.Смидович»
Н.В. Филимонова
от 28.06.2024 г. № 38

Сертификат: 00E719B594F57DA57381EAD5AC67BBA67C
Владелец: Филимонова Наталья Владимировна
Действителен: с 08.09.2023 до 01.12.2024

ИНСТРУКЦИЯ

по приему и сдаче помещений под охрану и правил допуска в помещения с установленными СКЗИ

1. Общие положения.

1.1. Помещения «МБДОУ Детский сад №6 п.Смидович» , в которых установлены криптосредства и его подразделений (отделов) относятся к категории защищаемых помещений. Помещения оснащены средствами пожарной и охранной сигнализаций с выводом ее на пульт охраны и/или в случае организации круглосуточной охраны внутри здания - под охрану дежурному поста охраны здания.

1.2. Дубликаты ключей от входных дверей помещений хранятся у дежурного поста охраны в опечатанном пенале.

2. Право самостоятельного доступ в помещения «МБДОУ Детский сад №6 п.Смидович» имеют:

- Руководитель «МБДОУ Детский сад №6 п.Смидович»;
- Заместитель руководителя «МБДОУ Детский сад №6 п.Смидович»;
- Документовед «МБДОУ Детский сад №6 п.Смидович».

3. Иные лица допускаются в помещение исключительно в присутствии работника, указанного в п.2 настоящей инструкции.

4. Вскрытие помещений может производиться только по согласованию и\или при участии ответственного за работу с СКЗИ. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещения посторонних лиц, информация незамедлительно сообщается руководителю структурного подразделения и\или ответственному за работу с СКЗИ. При необходимости составляется акт и принимаются меры к локализации последствий компрометации информации ограниченного доступа и к замене скомпрометированных криптоключей.

5. По окончании рабочего дня помещения и установленные в них хранилища должны быть закрыты.

Приложение 7

СПИСОК
пользователей СКЗИ имеющих право самостоятельного доступ в помещения,
в которых установлены СКЗИ.

№ п.п.	ФИО работника	Место нахождения помещения	Наименование помещения
1	Филимонова Наталья Владимировна	ЕАО, п.Смидович, ул.Комсомольская18	кабинет заведующего
2	Дмитрякова Наталья Григорьевна	ЕАО, п.Смидович, ул.Комсомольская,18	кабинет заведующего

Заведующий Н.В.Филимонова

Приложение 8

»

Журнал
учёта сейфов и ключей от них, а также ключа от помещения, где установлен СКЗИ .

№ п/п	Наименование хранилища	Заводской/ инвентарный номер хранилища	Расположение хранилища	Что хранится	Ф.И.О. ответственного за хранилище	Кол-во комплектов ключей и их номера	Расписка ответственного за хранилище в получении ключа и дата	Расписка в обратном приеме ключа и дата
1	2	3	4	5	6	7	8	9

В графе 1 указывается номер записи по порядку.

В графе 2 вносится наименование хранилища (сейф, металлический шкаф, кладовая, спецхранилище и т.п.).

В графе 3 вносится заводской/инвентарный номер или иной однозначно идентифицирующий хранилище номер.

В графе 4 вносится номер или название помещения, в котором установлено хранилище (подразделение, номер комнаты, корпуса, здания).

В графе 5 вносится информация о предметах защиты, находящихся в хранилище (документы, изделия, и т.п.).

В графе 6 вносится фамилия и инициалы лица, ответственного за хранилище.

В графе 7 вносится количество комплектов выданных ключей от хранилища и их номера.

В графе 8 вносится фамилия, инициалы, дата выдачи ключей и подпись лица, ответственного за хранилище.

В графе 9 вносится фамилия, инициалы, дата получения ключей и подпись лица, принявшего ключи от хранилища.

Приложение 9

Журнал
учёта обучения пользователей СКЗИ
в МБДОУ «Детский сад №6 п.Смидович»

№ п/п	ФИО пользователя СКЗИ	Должность	Отдел	Номер и дата заключения о допуске к СКЗИ	Период проведения обучения	Подпись обучаемого, дата	Подпись лица, проводившего обучение, дата
1	2	3	4	5	6	7	8
	Филимонова Наталья Владимировна	заведующий	МБДОУ «Детский сад №6 п.Смидович»				
	Дмитрякова Наталья Григоревна	заместитель заведующего	МБДОУ «Детский сад №6 п.Смидович»				

В графе 1 указывается номер записи по порядку.
В графе 2 вносится фамилия, инициалы обучаемого.
В графе 3 вносится должность обучаемого.
В графе 4 вносится отдел, в котором работает обучаемый.
В графе 5 вносится номер и дата заключения о допуске к СКЗИ.
В графе 6 вносится период проведения обучения.
В графе 7 вносится подпись обучаемого и дата.
В графе 8 вносится подпись лица, проводившего обучение и дата.

Приложение 10

Журнал
учета опломбирования СКЗИ, а также аппаратных средств, с которыми осуществляется функционирование СКЗИ

№ п/п	Имя (инвентарный/ серийный номер) СКЗИ/ аппаратного средства к которому подключено СКЗИ	Номер пломбы	Дата опломбирования	Ф.И.О. лица, проводившего опломбирование	Подпись	Дата снятия пломбы	Ф.И.О. лица, снявшего пломбу	Подпись
1	2	3	4	5	6	7	8	9

В графе 1 указывается порядковый номер в таблице.
В графе 2 указывается инвентарный номер аппаратного средства, но которое ставится или с которого снимается пломба.
В графе 3 вносится номер пломбы.
В графе 4 указывается дата опломбирования.
В графе 5 вносится фамилия, имя и отчество лица, проводившего опломбирование.
В графе 6 лицо, проводившее опломбирование, проставляет свою подпись после установки пломбы.
В графе 7 указывается дата снятия пломбы.
В графе 8 вносится фамилия, имя и отчество лица, снявшего пломбу.
В графе 9 лицо, проводившее снятие пломбы, проставляет свою подпись после снятия пломбы.

Приложение 11

Журнал
сдачи ключей от помещений и хранилищ документов
(типовая форма)

№№ п\п	Дата и время	Наименование помещения, его номер	Номер пломбы на пенале с ключами	Подпись сдавшего ключи	Подпись принявшего ключи	Дата и время	Подпись принявшего ключи обратно
1	2	3	4	5	6	7	8
1.							
2.							

В графе 1 указывается порядковый номер в таблице
В графе 2 указывается дата и время сдачи ключей
В графе 3 указывается наименование помещения, его номер
В графе 4 указывается номер пломбы лица, сдавшего пенал с ключами от помещения, указанного в графе № 3
В графе 5 указывается лицо, сдающее ключи, проставляет свою подпись после их сдачи
В графе 6 указывается лицо, принимающее ключи, проставляет свою подпись после их принятия
В графе 7 указывается дата принятия ключей
В графе 8 указывается лицо, принимающее ключи обратно, проставляет свою подпись после их принятия

Приложение 12

ЖУРНАЛ
поэкземплярного учета СКЗИ, эксплуатационной
и технической документации к ним, ключевых документов

Начат "_____"_____ 20__ г.
Окончен "_____"_____ 20__ г.

Ответственный за ведение: _____/_____/

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)		
				От кogovполучены или Ф.И.О. работника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и распискav в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводи-тельного письма	Дата и номер подтверждения или расписка в получении
1	2	3	4	5	6	7	8	9

Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
Дата и номер сопроводительного письма	Дата и номер подтверждения			Дата уничтожения	Номер акта или расписка об уничтожении	
10	11	12	13	14	15	16

Приложение 13

ЖУРНАЛ
учета личных печатей и пеналов

Начат "_____"_____ 20__ г.
Окончен "_____"_____ 20__ г.

Ответственный за ведение: _____/_____/

№ п/п	Оттиск печати	ФИО работника	Дата получения, Подпись	Дата сдачи, Подпись
1	2	3	4	5

Приложение 14

ТЕХНИЧЕСКИЙ (АППАРАТНЫЙ) ЖУРНАЛ
(типовая форма)

Начат "_____"_____ 20__ г.
Окончен "_____"_____ 20__ г.

Ответственный за ведение: _____/_____/

№ п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые крипто-ключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены крипто-ключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10

Приложение 15

АКТ №_____
установки и ввода в эксплуатацию СКЗИ
(типовая форма)

«___» _____ 20___г.

1. Комиссия в составе:
Председатель:
_____
Члены комиссии:
_____
_____
_____
составила настоящий Акт о том, что выполнены работы по установке средств криптографической защиты информации _____.

2. Выполнены работы по установке средств криптографической защиты информации в следующем объеме:

2.1. Установлены средства криптографической защиты информации: _____.

2.1.1. Тип СКЗИ: _____.

2.1.2. Регистрационный номер СКЗИ: _____.

2.1.3. Сертификат ФСБ России: №_____ от ___._____.20___, действителен до ___._____.20___.

2.1.4. Номер специального защитного знака (СЗЗ): _____.

2.1.5. Сертификат ФСТЭК России: №_____ от ___._____.20___, действителен до ___._____.20___.

2.1.6. Установка средств криптографической защиты информации выполнена с дистрибутива регистрационный (серийный) номер: _____.

2.2. Сведения о месте установки СКЗИ:

2.2.1. Наименование организации: _____.

2.2.2. Адрес установки СКЗИ: _____

2.2.3. Сведения о помещении: _____.

2.2.4. Серийный/инвентарный номер СКЗИ: _____.

2.2.5. Номер печатей (пломб) СКЗИ: _____.

2.3. Работы по установке СКЗИ выполнены в соответствии с: _____.

3. Проведена проверка целостности программного обеспечения и работоспособности программного (аппаратного, программно-аппаратного) _____.

4. Проведено обучение с принятием зачета по правилам эксплуатации, соблюдению требований безопасности при работе с программным комплексом и выполнению правил обращения с ключевыми носителями, а также об ответственности за их нарушение, пользователя СКЗИ:

4.1. Должность пользователя: _____.

4.2. Фамилия и инициалы: _____.

5. Помещение и его оборудование, размещение СКЗИ с установленным программным (аппаратным, программно-аппаратным) криптосредством, охрана помещения и подготовленность пользователя к самостоятельной эксплуатации средства криптографической защиты соответствуют требованиям «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», утвержденной приказом ФАПСИ от 13.06.2001 №152 и требованиям 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 защищённости».

6. Все технические и организационные меры для полноценной эксплуатации СКЗИ соблюдены. СКЗИ могут быть введены в эксплуатацию.

Председатель комиссии:

_____ _____

Члены комиссии:

_____ _____

_____ _____

_____ _____

Приложение 16

АКТ №_____
об уничтожении средств криптографической защиты информации, криптографических ключей, содержащихся на ключевых носителях, и ключевых документов
(типовая форма)

«___» _____ 20___г.

Комиссия в составе:
Председатель:
_____
Члены комиссии:
_____
_____
_____

произвела уничтожение: криптографических ключей, средства криптографической защиты информации, ключевые документы, дистрибутивы средств криптографической защиты информации (нужное подчеркнуть).

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Номера аппаратных средств, в которых установлены или к которым подключены СКЗИ	Номера экземпляров (криптографические номера) ключевых документов	Примечание

Всего уничтожено средств криптографической защиты информации, ключевых документов, дистрибутивов средств криптографической защиты информации (нужное подчеркнуть) _____.

Уничтожение: криптографических ключей, средств криптографической защиты информации, ключевых документов, дистрибутивов средств криптографической защиты информации (нужное подчеркнуть), выполнено путем: их стирания (разрушения), измельчения в шредере, (нужное подчеркнуть) по технологии, принятой для ключевых

носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Записи Акта сверены с записями Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Факт списания с учета ключевых носителей в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов подтверждаю:

Председатель комиссии:

_____ _____

Члены комиссии:

_____ _____

_____ _____

_____ _____

Приложение 17

Программа
обучения пользователей правилам работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну

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 с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13.06.2001 № 152.

2. Программа предназначена для обучения пользователей «НАИМЕНОВАНИЕ УЧРЕЖДЕНИЯ» правилам работы со средствами криптографической защиты информации (далее – СКЗИ), включающая следующий перечень тем занятий:

- Организация защиты информации при использовании СКЗИ (тема № 1);
- Требования к организации управления ключевой информацией СКЗИ (тема № 2);
- Криптография (тема № 3);
- Электронная подпись (тема № 4);
- Крипто Про CSP (тема № 5).

1. Содержание тем занятий

2.1. Организация защиты информации при использовании СКЗИ (тема № 1).

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

Нормативные правовые акты, регламентирующие правила работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну:

- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- 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»;

- приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- приказ ФАПСИ 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».

Для защиты информации необходимо проведение комплекса следующих мероприятий:

- 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 предприятия может быть различным по масштабам и формам. Это зависит в первую очередь от производственных, финансовых и иных возможностей организации, 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 предприятия.

Установление особого режима конфиденциальности.

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

Установление особого режима конфиденциальности включает в себя следующие действия:

- 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 работниками, 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.

Условия соблюдения особого режима конфиденциальности.

Требования к обеспечению установленного режима конфиденциальности оформляются в виде организационно-распорядительных документов и доводятся для ознакомления до работников учреждения.

Ограничение доступа к конфиденциальной информации способствует созданию наиболее эффективных условий ее сохранности. Необходимо определить список работников, допускаемых к конфиденциальной информации, с какими сведениями они могут работать и полномочия этих работников при работе с конфиденциальной информацией.

Для организации доступа к конфиденциальной информации ранее использовались организационные меры, основанные на строгом соблюдении работниками 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.

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 путем плановых и внеплановых проверок силами работников или с привлечением работников других организаций, которые специализируются в этой области. Также

проверки осуществляются на уровне межведомственного (государственного) контроля организациями, уполномоченными в сфере безопасности информации.

По результатам проверок специалистами по защите информации проводится необходимый анализ системы на соответствие требованиям с составлением отчета, который включает:

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

Необходимость создания органов защиты информации.

Для обеспечения и реализации перечисленных мероприятий (контроль, планирование и т.д.) требуется создание органа (службы) по защите информации. Эффективность защиты информации во многом будет определяться тем, насколько точно выбрана структура данного органа и уровнем квалификации его работников.

Органы защиты информации – это самостоятельные подразделения, но обычно ответственным за обеспечение защиты информации назначается один из штатных специалистов организации. Такая форма оправдана в тех случаях, когда объем необходимых мероприятий по защите информации небольшой и создание отдельного подразделения экономически невыгодно.

Средства защиты информации при передача 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 техническим каналам передачи данных осуществляется средствами криптографической защиты информации (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 электронной подписи и имитовставки).

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

2.2. Требования к организации управления ключевой информацией СКЗИ (тема № 2).

Хранение ключевых носителей.

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

Компрометация - факт доступа постороннего лица к защищаемой информации, а также подозрение на него. Чаще всего рассматривают компрометацию закрытого ключа, закрытого алгоритма, цифрового сертификата, учётных записей(паролей), абонентов или других защищаемых элементов, позволяющих удостоверить личность участника обмена информацией.

Если у пользователя появилось подозрение, что его персональный ключевой носитель попал, утерян, похищен, вышел из строя, скомпрометирован, он обязан немедленно прекратить (не возобновлять) работу с ключевым носителем, сообщить об этом администратору безопасности (работнику орган криптографической защиты информации (далее -ОКЗИ)), сдать ему скомпрометированную ключевой носитель, соблюдая обычную процедуру с пометкой в соответствующем журнале о причине возврата носителя, написать объяснительную записку о факте компрометации (поломки, утери, хищения) персонального ключевого носителя на имя начальника структурного подразделения.

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

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.

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.

Уничтожение ключевой информации на ключевых носителях.

Ключевая информация на ключевых носителях, срок эксплуатации которой истек, уничтожается согласно требований 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.

Учет пользовательской ключевой информации

В организации должен вестись «Журнал учета 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.

Рекомендации по размещению технических средств СКЗИ.

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

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 пользовательских ЭВМ (далее – ПЭВМ) одновременно может быть установлена только одна разрешенная операционная система (далее – 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 ISA и PCI устройств при использовании программно- аппаратного комплекса (далее – ПАК) защиты от несанкционированного доступа (далее - НСД), устанавливаемых в ISA и PCI разъем. Вход в BIOS ПЭВМ должен быть защищен паролем с длиной не менее 6 символов.

Организационные меры защиты информации от НСД.

При использовании СКЗИ должны соблюдаться следующие организационные меры:

1. Право доступа к рабочим местам с установленным СКЗИ предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе СКЗИ;
2. Запрещается осуществление несанкционированного Работником ОКЗИ 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, либо использовать ключевые носители на посторонних ПЭВМ;
5. Запрещается запись на ключевые носители посторонней информации;
6. На технических средствах, оснащенных СКЗИ, должно использоваться лицензионное ПО фирм-производителей;

7. 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;

8. 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;

9. Запрещается оставлять без контроля вычислительные средства (носители), которые эксплуатируются после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки;

10. Работником ОКЗИ должно быть проведено опечатывание системного блока с установленным СКЗИ, 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 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 системы или Работнику ОКЗИ;

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, 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;

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

Правила безопасности функционирования рабочих мест со встроенной СКЗИ.

1. Личные ключевые носители пользователей рекомендуется хранить в запираемом хранилище;

2. Рабочие места, на которые установлены СКЗИ, должны быть аттестованы комиссией. Результаты работы комиссии отражаются в «Акте готовности к работе» («Заключением о возможности эксплуатации СКЗИ»);

3. Правом доступа к рабочим местам с установленным СКЗИ должны обладать только лица, прошедшие соответствующую подготовку. Работник ОКЗИ должен ознакомить каждого пользователя, использующего СКЗИ, с настоящими Правилами пользования или с другими нормативными документами, созданными на их основе;

4. Должностные инструкции Работника ОКЗИ и ответственного исполнителя должны учитывать требования настоящих Правил;

5. 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;

6. Администратор безопасности (работник ОКЗИ) должен периодически (не реже чем раз в 6 месяцев) проводить контроль целостности и легальности установленных копий ПО на всех автоматизированных рабочих местах (АРМ) со встроенной СКЗИ с помощью программ контроля целостности;

7. В случае обнаружения «посторонних» (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на ПЭВМ 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 (пользователя), где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения;

8. Не допускается оставлять без контроля вычислительные средства, входящие в состав СКЗИ, при включенном питании и загруженном программном обеспечении СКЗИ. При кратковременном

перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана производится с использованием пароля доступа;

9. При каждом включении рабочей станции с установленным СКЗИ необходимо проверять сохранность печатей системного блока и разъемов рабочей станции;

10. Пользователь должен запускать только те приложения, которые разрешены администратором безопасности;

11. На ПЭВМ должна быть установлена только одна ОС;

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;

17. Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или контролирующими органами (администраторами безопасности, работниками ОКЗИ).

2.3. Криптография (тема № 3).

Криптография в современном мире

Поскольку ЭВМ 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.

Разновидности ключей

Еще одно деление криптоалгоритмов обычно основано на принципе использования ключа или ключей. При этом есть координальная 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. Мы 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 тп).

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 (тема № 4).

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).

При обмене электронными документами по сети связи существенно снижаются затраты на обработку и хранение документов, убыстряется их поиск. Но при этом возникает проблема аутентификации автора документа и самого документа, т.е. установления подлинности авторства и отсутствия изменений в полученном документе. В обычных (бумажных) документах эти проблемы решаются за счет того, что информация в документе и рукописная подпись автора жестко связаны с физическим носителем (бумагой). В электронных документах на машинных носителях такой связи нет. При обработке документов в электронной форме совершенно непригодны традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе.

В соответствии с Федеральным законом «Об электронной подписи» от 06.04.2011 № 63-ФЗ (далее – Федеральный закон № 63-ФЗ):

электронная подпись – это 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 либо доверенным лицом удостоверяющего центра 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 удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего

центра 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.

ЭП – 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.

ЭП равносильна собственноручной подписи владельца сертификата ключа проверки ЭП на бумажном документе при соблюдении некоторых простых условий.

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 изменение содержимое 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.

ЭП состоит из трех элементов:

- ключ ЭП – уникальная последовательность символов, предназначенная для создания электронной подписи;
- ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи;
- сертификат ключа проверки ЭП – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП.

Ключ ЭП и ключ проверки ЭП составляют ключевую пару ассиметричного шифрования.

ЭП обеспечивает:

- удостоверение источника документа. В зависимости от деталей определения «документа» могут быть подписаны такие поля, как автор, внесенные изменения, метка времени и т.д.;
- защиту от изменений документа. При любом случайном или преднамеренном изменении документа (или подписи) изменится хеш, следовательно, подпись станет недействительной;
- невозможность отказа от авторства. Так как создать корректную подпись можно лишь зная закрытый ключ (а он известен только владельцу), владелец не может отказаться от своей подписи под документом.

В соответствии с Федеральным законом № 63-ФЗ существуют следующие виды ЭП:

- простая ЭП;
- усиленная ЭП;
- усиленная квалифицированная ЭП (далее – квалифицированная ЭП).

Простой электронной подписью является ЭП, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования ЭП определенным лицом.

Неквалифицированной электронной подписью является ЭП, которая:

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

Квалифицированной электронной подписью является ЭП, которая соответствует всем признакам неквалифицированной ЭП и следующим дополнительным признакам:

- ключ проверки ЭП указан в квалифицированном сертификате;
- для создания и проверки ЭП используются средства ЭП, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом №63-ФЗ.

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

Согласно Федеральному закону № 63-ФЗ, электронный документ, подписанный простой или усиленной неквалифицированной ЭП, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью. При этом обязательным является соблюдение следующего условия: между участниками электронного взаимодействия должно быть заключено соответствующее соглашение.

Выделяются два формата ЭП:

CAdES BES – минимальный формат 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;

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

Дополнительно в состав ЭП 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 удостоверяющего центра, 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 ЭП будут вложены все доказательства, необходимые для проверки ее подлинности, то будет обеспечена офлайновая проверка подлинности вне зависимости от того, существует ли в момент проверки тот или иной УЦ, выдавший в свое время сертификат подписи. 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 (ЭДО) или как дополнительное средство обеспечения безопасности данных.

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

УЦ (удостоверяющий центр или центры), операторы ключевой системы, пользователи, на компьютере которых присутствует клиентское ПО для создания и проверки ЭП, а также носители, на которых сохранены индивидуальные наборы ключей.

2.5. КриптоПро CSP (тема № 5)

КриптоПро CSP – криптопровайдер, поддерживающий российские криптографические алгоритмы (ГОСТ), сертифицированный по требованиям ФСБ России к шифросредствам классов КС1, КС2, КС3 (требования к использованию различных классов описаны в приказе 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»).

Крипто Про CSP реализует следующие алгоритмы

ГОСТ 28147-89 –симметричное шифрование и имитовставка (MAC);

ГОСТ Р 34.11-94–функция хэширования;

ГОСТ Р 34.10-2001–электронная подпись, асимметричное шифрование.

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 34.102001 (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 дискеты нельзя.

Крипто Про CSP 4.0 :

текущая сертифицированная версия;

ключевые изменения по сравнению с 3.6.1: работа на Windows 7/8/8.1/10/Server 2003/2008 (x86, x64), на процессорах x64, расширен перечень поддерживаемых UNIX-платформ;

добавлена поддержка шифрование в соответствии с российским стандартом ГОСТ Р 34.102012, описывающим алгоритмы формирования и проверки электронной подписи;

поддерживается установка на КПК и смартфоны под управлением Windows Mobile.

Все версии Крипто Про CSP совместимы по форматам сообщений. Например, можно установить TLS-соединение с клиента версии 3.6.1 на сервер с версией 4.0. Аналогично, электронное письмо, зашифрованное и подписанное в версии 4.0 будет корректно расшифровано и проверено в версии 3.6.1.

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 (ГОСТ Р 34.10-2012) на различных ключевых носителях. Ключ на ключевом носителе может быть защищён паролем. Поддерживаются следующие типы носителей:

съёмные диски: дискета, USB флеш-накопитель и т.п.;

смарт-карты и USB-токены;

идентификаторы (таблетки) Touch Memory;

жёсткий диск или реестр Windows.

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.

Обратите 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 сертификат Удостоверяющего Центра.

Приложение 18

ЗАКЛЮЧЕНИЕ №___
о допуске к самостоятельной работе со средствами
криптографической защиты информации
(типовая форма)

«____» _____ 20___г.

Комиссия по допуску пользователей к самостоятельной работе с СКЗИ в составе:

Председатель:

_____ _____

Члены комиссии:

_____ _____

_____ _____

_____ _____

по результатам десятичасового обучения правилам работы со средствами криптографической защиты информации, в соответствии с Программой обучения работников правилам работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну, прошедшего с «____» _____ 20___ г. по «____» _____ 20 ___ г.,

РЕШИЛА:

Допустить пользователя_____

Должность: _____

Фамилия, имя, отчество: _____

к самостоятельной работе со средствами криптографической защиты информации в «НАИМЕНОВАНИЕ УЧРЕЖДЕНИЯ».

Председатель комиссии:

_____ _____

Члены комиссии:

_____ _____

_____ _____

_____ _____