ДЕПАРТАМЕНТ КУЛЬТУРЫ И ТУРИЗМА АДМИНИСТРАЦИИ ГОРОДА ЛИПЕЦКА
МУНИЦИПАЛЬНОЕ УЧРЕЖДЕНИЕ «ДОМ КУЛЬТУРЫ «МАТЫРА»

ПРИКАЗ

от «16» декабря 2025 г № 312

Липецк

О порядке хранения и эксплуатации средств криптографической защиты информации в муниципального учреждения «Дом культуры «Матыра»

В целях исполнения требований «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 июня 2001 г. № 152,

ПРИКАЗЫВАЮ:

1. Назначить ответственными за организацию работ по криптографической защите информации: заместителя директора Шокорова Д.А.
2. Утвердить:

2.1 Инструкцию ответственного за организацию работ по криптографической защите информации (Приложение № 1).

2.2 Положение об организации и проведении работ по обеспечению защиты информации с использованием средств криптографической защиты информации (далее – СКЗИ) (Приложение №2).

2.3 Программу обучения сотрудников муниципального учреждения «Дом культуры «Матыра» правилам работы со СКЗИ, не содержащей сведений, составляющих государственную тайну» (Приложение № 3).

2.4 Инструкцию пользователя средств криптографической защиты информации (Приложение № 4).

2.5 Перечень сотрудников, допущенных к работе с СКЗИ (Приложение № 5).

2.6 Форму Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Приложение № 6).

2.7 Форму Акта об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов (Приложение № 7).

2.8 Форму Журнала учета пользователей, прошедших обучение правилам работы с СКЗИ (Приложение № 8).

3. Ответственным за организацию работ по криптографической защите информации руководствоваться в своей деятельности Инструкцией ответственного за организацию работ по криптографической защите информации.

4. Ответственным за организацию работ по криптографической защите информации ознакомить под роспись пользователей со СКЗИ с Инструкцией пользователя средств криптографической защиты информации.
5. Ответственным за организацию работ по криптографической защите информации провести обучение пользователей правилам работы с СКЗИ согласно «Программы обучения сотрудников…», по окончании обучения данные пользователя внести в Журнал учета пользователей, прошедших обучение правилам работы с СКЗИ.
6. Контроль исполнения настоящего приказа оставляю за собой.

Директор
Муниципального учреждения
«Дом культуры «Матыра» Л.Л. Черепахина

Приложение № 1

к Приказу от «16» декабря 2025 г № 312

Инструкция
ответственного за организацию работ со средствами криптографической защиты информации

1. Общие положения

1.1. Настоящая Инструкция ответственного за организацию работ со средствами криптографической защиты информации в муниципальном учреждении «Дом культуры «Матыра» (далее – Инструкция) определяет основные обязанности и права ответственного за организацию работ со средствами криптографической защиты информации.

1.2. Ответственный за организацию работ со средствами криптографической защиты информации (далее – Ответственный за СКЗИ) отвечает за организацию, обеспечение функционирования и безопасности средств криптографической защиты информации, предназначенных для защиты информации, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация).

1.3. Ответственный за СКЗИ должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации, а также в области защиты информации при ее передаче по открытым каналам связи с использованием средств криптографической защиты.

1.4. В своей деятельности ответственный за СКЗИ руководствуется настоящей Инструкцией.

2. Обязанности ответственного за СКЗИ

Ответственный за СКЗИ обязан:

2.1. Соблюдать требования локальных актов, устанавливающих порядок работы с защищаемой информацией.

2.2. Проводить проверку готовности пользователей СКЗИ к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ.

2.3. Разрабатывать мероприятия по обеспечению функционирования и безопасности, применяемых СКЗИ, в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам.

2.4. Проводить обучение лиц, использующих СКЗИ, правилам работы с ними.

2.5. Осуществлять контроль за организацией, обеспечением функционирования и безопасности средств криптографической защиты информации, предназначенных для обеспечения защиты информации:

– контролировать соблюдение условий использования средств криптографической защиты информации (далее – криптосредства), предусмотренных эксплуатационной и технической документацией к ним;

– обеспечивать надежное хранение эксплуатационной и технической документации к криптосредствам, ключевым документам, носителям информации ограниченного распространения;

– вносить предложения по режиму охраны помещений, в которых установлены криптосредства или хранятся ключевые документы к ним;

– вести поэкземплярный учет СКЗИ, поступающих из сторонних организаций в «Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (для ответственного за СКЗИ)»;

– выдавать пользователям средств криптографической защиты информации экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевые документы под расписку в «Журнале поэкземплярного учета средств криптографической

защиты информации, эксплуатационной и технической документации к ним, ключевых документов (для пользователей СКЗИ)»;

– контролировать передачу криптосредств, эксплуатационной и технической документации к ним, ключевых документов между пользователями средств криптографической защиты информации и (или) ответственным за организацию работ со средствами криптографической защиты информации под расписку в соответствующем Журнале;

– пломбировать (опечатывать) и контролировать сохранность печатей (пломб) на аппаратных средствах, с которыми осуществляется штатное функционирование криптосредств, а также аппаратных и аппаратно-программных криптосредствах;

– контролировать получение и доставку криптосредств, эксплуатационной и технической документации к ним;

– заблаговременно делать заказы на изготовление очередных ключевых документов и рассылку на места использования для своевременной замены действующих ключевых документов;

– контролировать уничтожение неиспользованных или выведенных из действия ключевых документов в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам, или, если срок уничтожения эксплуатационной и технической документацией не установлен, не позднее 10 суток после вывода их из действия (окончания срока действия) под расписку в соответствующем Журнале;

– выводить из действия носители ключевой информации (далее – НКИ), в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие НКИ;

– принимать решение в чрезвычайных случаях, когда отсутствуют НКИ для замены скомпрометированных, об использовании скомпрометированных НКИ;

– проводить инструктаж пользователей средств криптографической защиты информации по правилам работы с криптосредствами и ключевыми документами;

2.6. Требовать прекращения обработки защищаемой информации в случае нарушения установленного порядка работ с криптосредствами или нарушения функционирования криптосредств.

2.7. Участвовать в анализе ситуаций, касающихся нарушения условий хранения носителей защищаемой информации, использования криптосредств, которые могут привести к нарушению конфиденциальности защищаемой информации.

2.8. Контролировать исполнение пользователями средств криптографической защиты информации требований «Инструкции пользователя СКЗИ», а также требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения защиты информации.

2.9. Принимать все необходимые меры для обеспечения защиты информации, в случае получения от пользователей информации о фактах утраты, компрометации ключевой информации, в частности, обеспечить выполнение следующих мероприятий:

– в каждом случае, по факту (или предполагаемой) компрометации ключевых документов, проводится служебное расследование; результатом расследования является квалификация или не квалификация данного события как компрометация;

– о факте компрометации ключевой информации пользователями средств криптографической защиты информации совместно с администратором безопасности производится информирование всех заинтересованных участников информационного обмена;

– выведенные из действия скомпрометированные ключевые документы после проведения расследования уничтожаются, о чем делается соответствующая запись в Журнале;

– для своевременного восстановления связи пользователю средств криптографической защиты информации выдается новый НКИ; для этого создаётся

резервный запас НКИ, использование которых осуществляется в случаях крайней необходимости по решению ответственного за СЗКИ.

2.10. Подготавливать копии НКИ, которые подлежат основному учету и хранятся в сейфе ответственного за организацию работ со средствами криптографической защиты информации. Данные копии применяются с разрешения руководителя организации или другого уполномоченного лица, если по результатам расследования не было установлено факта компрометации.

2.11. Хранить резервные НКИ отдельно от рабочих (актуальных) НКИ, с целью обеспечения невозможности их одновременной компрометации.

2.12. Своевременно информировать администратора безопасности о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемой информации.

3. Права ответственного за организацию работ со средствами криптографической защиты информации

Ответственный за организацию работ со средствами криптографической защиты информации имеет право:

3.1. Знакомиться с локальными актами, регламентирующими процессы обработки защищаемой информации.

3.2. Требовать от пользователей СКЗИ соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения защиты информации.

3.3. Требовать прекращения работы в случае выявления нарушений требований по работе с криптосредствами, предназначенными для обеспечения защиты информации, или в связи с нарушением функционирования криптосредств.

Приложение № 2

к Приказу от «16» декабря 2025 г № 312

Положение
об организации и проведении работ по обеспечению защиты информации с использованием средств криптографической защиты

1. Общие положения

1.1. Настоящий порядок разработан для практического применения пользователями средств криптографической защиты информации в муниципальном учреждении «Дом культуры «Матыра» (далее – Организация) 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 РФ от 13.06.2001 № 152, «Типовых требований 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», утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622, Приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.2. Должностные лица, ответственные за обеспечение защиты информации и эксплуатации СКЗИ назначается приказом руководителя Организации.

1.3. В Организации разрабатываются нормативные и распорядительные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ.

2. Термины и определения

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

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

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

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

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

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

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

3. Порядок обращения с конфиденциальной информацией

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

3.1. Информация, полученная сотрудниками при регистрации пользователя, является конфиденциальной и не подлежит разглашению третьим лицам.

3.2. Конфиденциальная информация, полученная сотрудниками, в результате выполнения должностных обязанностей в процессе работы с СКЗИ, должна сохраняться в тайне.

3.3. Содержание закрытых ключей СКЗИ и ключевых документов должно сохраняться в тайне.

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

3.5. Не допускается:

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;

– вставлять ключевой носитель в ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.), а также в дисководы других ПЭВМ;

– записывать на ключевом носителе постороннюю информацию;

– вносить какие-либо изменения в ПО СКЗИ и ключевую информацию;

– модифицировать содержимое ключевых носителей; использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования;

– снимать несанкционированные копии с ключевых носителей; знакомить кого-либо с содержанием ключевых носителей или передавать кому-либо ключевые носители.

4. Требования по размещению СКЗИ и режиму охраны

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

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

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

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

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

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

4.7. Технические средства с СКЗИ оборудуются средствами контроля вскрытия (опломбируются).

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

5. Требования по обеспечению безопасности СКЗИ и ключевой информации

5.1. Ключевые и инсталляционные носители с программным обеспечением СКЗИ берутся на поэкземплярный учет в выделенных для этих целей журналах.

5.2. Учет и хранение ключевых носителей поручается специально выделенным сотрудникам.

5.3. Для хранения ключевых носителей выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации.

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

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

6. Порядок допуска к самостоятельной работе с СКЗИ

6.1. К самостоятельной работе с СКЗИ допускаются лица, назначенные на должности, выполнение обязанностей по которым связано с хранением и использованием СКЗИ.

6.2. Сотрудники допускаются к самостоятельной работе с СКЗИ после их специальной подготовки (обучения) по утвержденным.

6.3. Программа подготовки к самостоятельной работе с СКЗИ (Приложение) содержит:

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

Приложение № 3

к Приказу от «16» декабря 2025 № 312

ПРОГРАММА

обучения сотрудников муниципальном учреждении «Дом культуры «Матыра» 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 содержащих сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ РФ от 13.06.2001 № 152.

1.2. Программа предназначена для обучения пользователей СКЗИ муниципальном учреждении «Дом культуры «Матыра», а также пользователей СКЗИ – сотрудников организаций в рамках заключенных договоров по защищенному обмену электронными документами.

2. Темы занятий

2.1. Организация защиты информации при использовании СКЗИ

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

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»;
- 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»;
- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ РФ от 13.06.2001 № 152.
- «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение «ПКЗ-2005») (утверждено Приказом ФСБ от 9 февраля 2005г. № 66).

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

Для защиты информации в организации необходим целый комплекс мероприятий по ее защите. Это:

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

Установление особого режима конфиденциальности.

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

Как правило, установление особого режима конфиденциальности включает в себя:

–организацию охраны помещений, в которых содержатся носители конфиденциальной информации;

–установление режима работы в помещениях, в которых содержатся носители конфиденциальной информации;

–установление пропускного режима в помещения, содержащие носители конфиденциальной информации;

–закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;

–установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);

–организацию ремонта технических средств обработки конфиденциальной информации;

– организацию контроля за установленным порядком.

Условия соблюдения особого режима конфиденциальности.

Требования к выполнению установленного режима конфиденциальности оформляются в виде организационно-распорядительных документов и доводятся для ознакомления до сотрудников предприятия.

Ограничение доступа к конфиденциальной информации способствует созданию наиболее эффективных условий сохранности конфиденциальной информации. Необходимо четко определять круг сотрудников, допускаемых к конфиденциальной информации, к каким конкретно сведениям им разрешен доступ и полномочия сотрудников по доступу к конфиденциальной информации. Традиционно для организации доступа к конфиденциальной информации использовались организационные меры, основанные на строгом соблюдении сотрудниками процедур допуска к информации, определяемых соответствующими инструкциями, приказами и другими нормативными документами.

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

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.

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

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

– вывод о соответствии проводимых на предприятии мероприятий установленным требованиям;

– оценка реальной эффективности применяемых на предприятии мер защиты информации и предложения по их совершенствованию.

Средства защиты информации при передаче ее по каналам связи.

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

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

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

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

2.2. Требования к организации управления ключевой информацией СКЗИ

Хранение ключевых носителей.

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

При централизованном хранении ключевых носителей администратор безопасности и ответственный за организацию работ со средствами криптографической защиты информации несут персональную ответственность за хранение личных ключевых носителей пользователей. Личные ключевые носители администратора безопасности должны хранится в его личном сейфе.

Сроки действия ключей.

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

Сроки действия системной ключевой информации как правило, не должны превышать 3-5 лет.

Уничтожение ключевой информации на ключевых носителях.

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

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

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 тексту – 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 ПЭВМ одновременно может быть установлена только одна разрешенная ОС.

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

Средствами BIOS должна быть исключена возможность отключения пользователями ISA и PCI устройств при использовании ПАК защиты от 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 ПО СКЗИ предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе СКЗИ.
2. Запрещается осуществление несанкционированного администратором безопасности копирование ключевых носителей.
3. Запрещается разглашение содержимого ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер.
4. Запрещается использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ, либо использовать ключевые носители на посторонних ПЭВМ.
5. Запрещается запись на ключевые носители посторонней информации.
6. На технических средствах, оснащенных СКЗИ, должно использоваться только лицензионное программное обеспечение 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, которые эксплуатируются после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.
10. 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.
11. 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.

12. 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.

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

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

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

16. При загрузке ОС должен производиться контроль целостности программного обеспечения, входящего в состав СКЗИ, самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ.

17. Должно производиться физическое затирание содержимого удаляемых файлов.

18. Должны быть реализованы организационно-технические меры защиты.

Правила безопасности функционирования рабочих мест со встроенной СКЗИ.

1. Личные ключевые носители пользователей рекомендуется хранить в сейфе.
2. Правом доступа к рабочим местам с установленным СКЗИ должны обладать только лица, прошедшие соответствующую подготовку. Администратор информационной безопасности должен ознакомить каждого пользователя, использующего СКЗИ, с настоящими Правилами пользования или с другими нормативными документами, созданными на их основе.
3. Должностные инструкции администратора информационной безопасности и ответственного исполнителя должны учитывать требования настоящих Правил.
4. Системные блоки ПЭВМ с установленным СКЗИ должны быть опечатаны специально выделенной для этих целей печатью. Наряду с этим допускается применение других дополнительных средств контроля за доступом к ПЭВМ.
5. Администратор информационной безопасности должен проводить контроль целостности и легальности установленных копий ПО на всех АРМ со встроенной СКЗИ с помощью программ контроля целостности.
6. В случае обнаружения "посторонних» (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией в составе представителей служб информационной безопасности организации - владельца сети и организации - абонента сети (пользователя), где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения.
7. Не допускается оставлять без контроля вычислительные средства, входящие в состав СКЗИ, при включенном питании и загруженном программном обеспечении СКЗИ. При кратковременном перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана производится с использованием пароля доступа.
8. При каждом включении рабочей станции с установленным СКЗИ необходимо проверять сохранность печатей системного блока и разъемов рабочей станции.
9. Пользователь должен запускать только те приложения, которые разрешены администратором безопасности.
10. На ПЭВМ должна быть установлена только одна ОС.
11. ПО, установленное на ПЭВМ, не должно иметь встроенных средств разработки и отладки программ.

12. Должны быть приняты меры по исключению вхождения пользователей в режим конфигурирования BIOS (например, с использованием парольной защиты).
13. Должна быть исключена возможность работы на ПЭВМ, если во время начальной загрузки не проходят встроенные тесты.
14. Пароли, назначаемые пользователям, должны отвечать требованиям соответствующих инструкции и нормативных документов (ГТК, ЦБ РФ).
15. 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).

2.3. Криптография

Криптография в современном мире

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

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

Симметричные криптосистемы

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

Блочные, потоковые и гибридные системы

Самое общепринятое деление криптоалгоритмов организовано по их методу обработки информации.

Блочные крипто алгоритмы

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 кардинальная разница между симметричным криптоалгоритмом и симметричным ключом. Симметричный ключ является всего лишь одним из вариантов реализации симметричного криптоалгоритма, хотя данный вариант является самым распространенным, есть и другие реализации использования ключей. 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 т.п).

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

Криптоанализ делят на линейный и дифференциальный.

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

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

Распространенные алгоритмы

- AES (англ. Advanced Encryption Standard) -американский стандарт шифрования;
- ГОСТ 34.12-2018 – отечественный стандарт шифрования данных (описывает шифры «Магма» и «Кузнечик»);
- DES (англ. Data Encryption Standard) -стандарт шифрования данных в США до AES;
- 3DES (Triple-DES, тройной DES);
- RC6 (Шифр Ривеста);
- Twofish;
- IDEA (англ.International Data Encryption Algorithm);
- SEED - корейский стандарт шифрования данных;
- Camellia - сертифицированный для использования в Японии шифр;
- CAST (по инициалам разработчиков Carlisle Adams и Stafford Tavares);
- XTEA - наиболее простой в реализации алгоритм.

2.4. Электронная подпись

При постепенном переводе данных в электронный вид, встал вопрос не только о сохранении конфиденциальности документа (применением шифрования), целостности документа (применением хэширования), но также и привязке документа к человеку и однозначное отношение этого человека к документу. Эти требования к электронному

документообороту носят название подтверждение авторства и невозможность отказа от авторства. Именно их реализует электронная подпись (далее – ЭП).

В соответствии с Федеральным законом «Об электронной подписи» от 06 апреля 2011 года № 63-ФЗ **электронная подпись** - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром 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);

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.

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

Электронная подпись – это эффективное средство защиты информации от модификации, которое переносит свойства реальной подписи под документом в область электронного документооборота. В основу ЭП положены такие криптографические методы, как асимметричное шифрование и хэш-функции.

Процесс ЭП использует криптографические преобразования для создания самого ЭП, несущего дополнительную информацию об авторе, времени подписи и иногда о назначении подписи (зависит от клиентской среды документооборота).

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

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

Первичная ЭП, которой заверяется и защищается от изменений 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.

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

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

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

Выделяются два формата ЭП:

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

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

В число дополнений входят:

штамп времени - подписанный ЭП документ, которым служба штампов времени удостоверяет, что в указанный момент времени ей было предоставлено значение хеш-функции от другого документа. Само значение хеш-функции также указывается в штампе времени. Предоставляется службой штампов времени (TSA), компонентом удостоверяющего центра, обладающим точным и надежным источником времени и предоставляющим услуги по созданию штампов времени;

цепочки сертификатов до доверенного Удостоверяющего центра и OCSP-ответов. На эти данные также получается штамп времени, подтверждающий их целостность в момент проверки.

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

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

Приложение № 4

к Приказу от «16» декабря 2025 г № 312

ИНСТРУКЦИЯ
пользователя средств криптографической защиты информации

1. Общие положения

1.1. Настоящая Инструкция пользователя средств криптографической защиты информации (далее – СКЗИ) (далее – Инструкция) определяет права и обязанности пользователей СКЗИ, порядок обращения со СКЗИ, а также определяет порядок восстановления связи в случае компрометации действующих ключей к СКЗИ.

1.2. Пользователем СКЗИ является лицо, назначенное на должность, выполнение обязанностей по которой связано с изготовлением, хранением и использованием СКЗИ.

1.3. Пользователь СКЗИ должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения защиты информации, а также в области защиты информации при ее передаче по открытым каналам связи с использованием средств криптографической защиты.

1.4. Пользователи СКЗИ несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту СКЗИ от несанкционированного использования.

2. Обязанности и права пользователя СКЗИ

2.1. Пользователь СКЗИ обязан:

– обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей;

– соблюдать требования по обеспечению безопасности функционирования СКЗИ;

– немедленно уведомлять администратора безопасности и ответственного за организацию работ со средствами криптографической защиты информации о компрометации носителя ключевой информации, о фактах утраты или недостачи СКЗИ;

– в пределах своей компетенции предоставлять информацию комиссии, проводящей служебные расследования по фактам компрометации, а также выявлению причин нарушения требований безопасности функционирования СКЗИ;

– сдать ответственному за организацию работ со средствами криптографической защиты информации носители ключевой информации при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– сдать ответственному за организацию работ со средствами криптографической защиты информации носитель ключевой информации по окончании срока действия сертификата ключа, а также в случае компрометации ключа.

2.2. Пользователю СКЗИ запрещается:

– осуществлять несанкционированное и безучётное копирование ключевых данных;

– хранить носители ключевой информации вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность;

– передавать носители ключевой информации каким бы то ни было лицам, кроме ответственного за организацию работ со средствами криптографической защиты информации;

– во время работы оставлять носитель ключевой информации без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ);

– хранить на носителе ключевой информации какую-либо информацию, кроме ключевой;

– использовать в помещениях, где применяются СКЗИ, личные технические средства, позволяющие осуществлять копирование ключевой информации;

– использовать носители ключевой информации, выведенные из действия.

2.3. Пользователь имеет право:

– вносить предложения руководству по вопросам использования СКЗИ;

– повышать уровень квалификации по использованию СКЗИ.

3. Порядок обращения со СКЗИ

3.1. Для хранения носителя ключевой информации пользователь СКЗИ должен быть обеспечен личным сейфом.

3.2. Дубликаты ключей от сейфов пользователей СКЗИ должны храниться в сейфе ответственного за организацию работ со средствами криптографической защиты информации. Несанкционированное изготовление дубликатов ключей запрещено. В случае утери ключа механизм замка (либо сам сейф) должен быть заменён.

3.3. К эксплуатации СКЗИ допускаются лица, прошедшие соответствующую подготовку и изучившие правила пользования данным СКЗИ.

3.4. Все программное обеспечение ПЭВМ, предназначенное для установки СКЗИ, должно иметь соответствующие лицензии.

4. Восстановление связи в случае компрометации действующих ключей к СКЗИ

4.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию владельца носителя ключевой информации и конфиденциальность информации, обрабатываемой с его помощью.

4.2. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

– утрата (хищение) носителя ключевой информации, в том числе – с последующим их обнаружением;

– увольнение (переназначение) сотрудников, имевших доступ к носителю ключевой информации;

– передача секретных ключей по линии связи в открытом виде;

– нарушение правил хранения носителя ключевой информации;

– вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

– ошибки при совершении криптографических операций;

– несанкционированное или безучётное копирование ключевой информации;

– все случаи, когда нельзя достоверно установить, что произошло с носителем ключевой информации (в том числе случаи, когда носитель ключевой информации вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

4.3. При наступлении любого из перечисленных выше событий пользователь СКЗИ или владелец носителя ключевой информации должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) ответственному за организацию работ со средствами криптографической защиты информации лично, по телефону, электронной почте или другим доступным способом. В любом случае пользователь СКЗИ или владелец носителя ключевой информации обязан убедиться, что его сообщение получено и прочтено.

4.4. При подтверждении факта компрометации действующих ключей пользователь СКЗИ обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей и сдачу ответственному за организацию работ со средствами криптографической защиты информации в течение 3 рабочих дней.

4.5. Для восстановления конфиденциальной связи после компрометации действующих ключей пользователь СКЗИ получает у ответственного за организацию работ со средствами криптографической защиты информации новые ключи.

Приложение № 6

к Приказу от «16» декабря 2025 г № 312

ФОРМА

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

№	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 ключевых документов	Отметка о получении	
				От кого получены	Дата и номер сопроводительного письма.
	2.	3.	4.	5.	6.

Отметка о выдаче		Отметка о подключении (установке) СКЗИ		
Ф.И.О пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. сотрудника, проводившего установку	Дата установки и подписи лиц, произведших установку	Номера аппаратных средств, в которые установлены СКЗИ
7.	8.	9.	10.	11.

Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Дата изъятия (уничтожения)	Ф.И.О. сотрудника, проводившего изъятие (уничтожение) СКЗИ	Номер Акта или расписка об уничтожении	
12.	13.	14.	15.

Приложение № 7

к Приказу от «16» декабря 2025 г № 312

ФОРМА

АКТ №_____
об уничтожении криптографических ключей и ключевых документов.

г. _____ **« »_____20__г.**

Комиссия в составе:
Председателя: _____, членов комиссии:
_____
_____

произвела уничтожение криптографических ключей и ключевых документов:

№ п/п	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего уничтожается ключей (документов)	Примечание
1	2	3	4	5	6	7	8

Всего уничтожено (_____) криптографических ключей на (_____) ключевых носителях. Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Уничтожение криптографических ключей выполнено путем их стирания в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Ключевые носители списаны с учета в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/
_____ /_____/
_____ /_____/

Приложение № 8

к Приказу от «16» декабря 2025 г № 312

ФОРМА

ЖУРНАЛ
учета пользователей, прошедших обучение правилам работы с СКЗИ

№	ДОЛЖНОСТЬ	Ф.И.О. ПОЛЬЗОВАТЕЛЯ СКЗИ	ПРОГРАММА ОБУЧЕНИЯ	ДАТА ПРОВЕДЕНИЯ ОБУЧЕНИЯ	ПОДПИСЬ ОБУЧЕМОГО, ДАТА	ПОДПИСЬ ПРОВОДИВШЕГО ОБУЧЕНИЕ, ДАТА