АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ СЕВЕРСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН КРАСНОДАРСКОГО КРАЯ

П О С Т А Н О В Л Е Н И Е

от 04.07.2025 № 1137

станица Северская

Об утверждении Политики использования средств криптографической защиты информации администрации муниципального образования Северский муниципальный район Краснодарского края

В целях повышения уровня защиты информации в администрации муниципального образования Северский муниципальный район Краснодарского края, в соответствии с приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 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», положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты, утверждённым приказом ФСБ России от 9 февраля 2005 года № 66, 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, утверждённой приказом Федерального агентства правительственной связи и информации Российской Федерации от 13 июня 2001 года № 152, методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах

персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утверждёнными руководством 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432, руководствуясь статьями 31, 66 Устава муниципального образования Северский муниципальный район Краснодарского края, п о с т а н о в л я ю:

1. Утвердить Политику использования средств криптографической защиты информации администрации муниципального образования Северский муниципальный район Краснодарского края (далее – Администрация) (приложение).

2. Управлению информатизации и информационной безопасности (Сергиевская Н.Н.):

1) опубликовать настоящее постановление на официальном Интернет-портале Администрации в разделе «Информатизация»;

2) ознакомить под подпись с настоящим постановлением сотрудников Администрации, обрабатывающих персональные данные в Администрации.

3. Управлению по связям с общественностью (Поляшенко Е.А.) разместить настоящее постановление на официальном сайте Администрации в информационно-телекоммуникационной сети «Интернет» в разделе «Муниципальные правовые акты».

4. Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Разумца В.М.

5. Постановление вступает в силу со дня его подписания.

Исполняющий
обязанности главы
муниципального
образования
Северский
муниципальный район
Краснодарского края

Подлинник электронного документа, подписанного электронной подписью, хранится в системе электронного документооборота администрации МО Северский район Краснодарского края
Сертификат 00BA269C5AD300FFCFF996FECC964FDADC
Владелец **Малов Дмитрий Андреевич**
Действителен с 12.08.2024 по 05.11.2025

Д.А. Малов

Приложение

УТВЕРЖДЕНА
постановлением администрации
муниципального образования
Северский муниципальный район
Краснодарского края
от _____№_____

ПОЛИТИКА
использования средств криптографической защиты информации администрации муниципального образования Северский муниципальный район

1. Общие положения

1.1. Политика использования средств криптографической защиты информации (далее – Политика) администрации муниципального образования Северский муниципальный район (далее – Администрация) определяет:

порядок учёта, хранения и использования средств криптографической защиты информации (далее – СКЗИ), криптографических ключей и эксплуатационной документации к ним;

порядок действий по уничтожению криптографических ключей;

порядок действий при компрометации криптографических ключей.

1.2. Настоящая политика разработана в соответствии с:

приказом Федеральной службы безопасности Российской Федерации (далее – ФСБ России) от 10 июля 2014 года № 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»;

положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (далее - Положение ПКЗ-2005), утверждённым приказом ФСБ России от 9 февраля 2005 года № 66;

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, утверждённой приказом Федерального агентства правительственной связи и информации Российской Федерации от 13 июня 2001 года № 152 (далее – ФАПСИ);

методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных,

эксплуатируемых при осуществлении соответствующих видов деятельности, утверждёнными руководством 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432.

1.3. К средствам криптографической защиты информации относятся:

реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при её обработке, хранении и передаче по каналам связи, включая СКЗИ;

реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при её обработке и хранении;

реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и электронной подписи;

аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ, независимо от вида носителя ключевой информации.

1.4. Использование СКЗИ для обеспечения безопасности информации необходимо в следующих случаях:

если защищаемая информация подлежит криптографической защите в соответствии с законодательством Российской Федерации;

если в информационных системах существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ;

если в Администрации принято решение о необходимости применения криптографической защиты информации.

1.5. К случаям, когда угрозы безопасности информации могут быть нейтрализованы только с помощью СКЗИ, относятся:

передача защищаемой информации по каналам связи, не защищённым от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче персональных данных по информационно-телекоммуникационным сетям общего пользования);

хранение защищаемой информации на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключён без применения криптографических способов защиты информации.

1.6. Для обеспечения безопасности информации при её обработке в информационных системах должны использоваться СКЗИ, сертифицированные ФСБ России по требованиям, предъявляемым к СКЗИ. Необходимый к использованию класс СКЗИ определяется по результатам определения угроз (возможностей потенциальных нарушителей) СКЗИ.

2. Правила ввода СКЗИ в эксплуатацию

2.1. При вводе СКЗИ в эксплуатацию должны соблюдаться следующие правила:

осмотр СКЗИ, дистрибутивов на факт наличия физических дефектов, наличие заводских пломб, наличие эксплуатационной и технической документации к поставляемому СКЗИ, отсутствие признаков компрометации;

сверка акта приема передачи поставляемых СКЗИ (при наличии);

установка и ввод в эксплуатацию СКЗИ осуществляется в соответствии с эксплуатационной и технической документацией;

по результатам настройки и установки составляется «Акт установки и ввода в эксплуатацию СКЗИ» (Форма Акта установки и ввода в эксплуатацию СКЗИ приведена в приложении 1 к настоящей политике);

производится обучение работников работе с СКЗИ;

составляется протокол принятия зачета у пользователя СКЗИ (форма протокола принятия зачета у пользователя СКЗИ приведена в приложении 2 к настоящей политике);

оформляется лицевой счет пользователя (форма лицевого счета пользователя СКЗИ приведена в приложении 3 к настоящей политике);

орган криптографической защиты информации (далее - ОКЗИ) выдает заключение о допуске пользователя к самостоятельной работе с СКЗИ (форма заключения о допуске пользователя к самостоятельной работе с СКЗИ приведена в приложении 4 к настоящей политике);

допускается возложение функций ОКЗИ на специальное структурное подразделение по защите государственной тайны, использующее для этого шифровальные средства;

производится запись в технический (аппаратный) журнал (приложение 5),

журнал поэкземплярного учёта СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал учёта СКЗИ) (в приложении 8),

акт уничтожения СКЗИ (в приложении 6), журнал учёта

хранилищ СКЗИ и ключей от них (в приложение 7).

3. Организация передачи информации по каналам связи с использованием СКЗИ защищаемой информации

3.1. Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ защищаемой информации организуется и обеспечивается на основании договоров на оказание услуг по криптографической защите информации организациями, имеющими лицензию ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных

(криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)[1]) (далее – лицензиаты ФСБ России). За исключением случаев, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд Администрации.

3.2. Для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ защищаемой информации в соответствие с пунктом 6 Приказа ФАПСИ, лицензиат ФСБ России создаёт орган криптографической защиты информации (специальное структурное подразделение).

3.3. Орган криптографической защиты информации или специальное структурное подразделение осуществляет:

установку и настройку программных и программно-аппаратных средств криптографической защиты информации;

подготовку к вводу в эксплуатацию СКЗИ в соответствии с требованиями эксплуатационной документации.

Установка и ввод в эксплуатацию СКЗИ производится на основании «Акта установки и ввода в эксплуатацию средства криптографической защиты информации», который утверждается главой муниципального образования Северский муниципальный район;

проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием типа и номеров, используемых СКЗИ, номеров аппаратных, программных и аппаратно-программных средств, где установлены или к которым подключены СКЗИ, с указанием также номеров печатей, которыми опечатаны технические средства, включая СКЗИ, и результатов проверки функционирования СКЗИ);

разработку мероприятий 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;

инструктаж лиц, использующих СКЗИ, по правилам работы с ними;

поэкземплярный учёт используемых СКЗИ, эксплуатационной и технической документации к ним;

учёт обслуживаемых обладателей конфиденциальной информации, а также физических лиц, непосредственно допущенных к работе с СКЗИ;

контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ;

расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты

---

1) В лицензии должны быть указаны пункты:12,13,14,15, 17, 18, 20, 21, 22, 23, 24 согласно Постановления Правительства РФ от 16.04.2012 № 313.

информации; разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

разработку схемы организации криптографической защиты информации (с указанием наименования, обладателей конфиденциальной информации, типов, применяемых СКЗИ и ключевых документов к ним, видов защищаемой информации, используемых совместно с СКЗИ технических средств связи, прикладного и общесистемного программного обеспечения, и средств вычислительной техники).

3.4. Обладатель конфиденциальной информации, владеющий СКЗИ, осуществляет:

поэкземплярный учёт и хранение СКЗИ согласно разделу 4 настоящей политики;

работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (только для обеспечения собственных нужд Администрации), в соответствии с требованиями разделов 5, 8, 10 настоящей политики.

4. Учёт и хранение СКЗИ и криптографических ключей к ним

4.1. Средства криптографической защиты информации, криптографические ключи (ключевые документы), а также эксплуатационная и техническая документация к СКЗИ, подлежат поэкземплярному учёту.

4.2. Поэкземплярный учёт СКЗИ ведётся в Журнале учёта СКЗИ, при этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

4.3. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов выдаются под расписку в Журнале учёта СКЗИ, лицам, несущим персональную ответственность за их сохранность. Единицей поэкземплярного учёта ключевых документов считается ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

4.4. Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей, или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, который ведет ответственный пользователь СКЗИ.

4.5. Передача СКЗИ, эксплуатационной и технической, ключевых документов допускается только между пользователями СКЗИ под расписку в журнале поэкземплярного учёта.

4.6. Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к СКЗИ хранятся у администратора информационной безопасности, в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. Администратор информационной безопасности также обязан

предусмотреть раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей.

4.7. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны). Место опечатывания СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. Пользователь СКЗИ должен периодически проверять сохранность оборудования и целостность печатей на автоматизированных рабочих местах (далее – АРМ) и серверах, в которых установлены СКЗИ. В случае обнаружения посторонних (незарегистрированных) программ или выявления факта повреждения печати работа должна быть прекращена. По данному факту проводится служебное расследование и осуществляются работы по анализу и ликвидации последствий данного нарушения (регистрируется инцидент информационной безопасности).

4.8. СКЗИ и криптографические ключи могут в случае необходимости пересылаться специальной (фельдъегерской) связью или со специально выделенными нарочными (из числа работников Администрации, лиц, имеющих доверенность на право получения СКЗИ) при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ и криптографическим ключам во время доставки.

4.9. Для пересылки СКЗИ криптографические ключи помещаются в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия. Криптографические ключи пересылают в отдельном пакете с пометкой «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

4.10. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, криптографических ключей составляется Акт приёма-передачи (Опись) документов, в котором указывается: что посылается и в каком количестве, учётные номера СКЗИ, криптографических ключей или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Акт приёма-передачи (Опись) документов вкладывается в упаковку.

4.11. Полученную упаковку вскрывает только лицо, для которого она предназначена. Если содержимое полученной упаковки не соответствует указанному в Акте приёма-передачи (Описи) документов, или сама упаковка и печать их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к её содержимому, то получатель составляет акт, который высылается отправителю. Полученные с такими отправлениями СКЗИ и криптографические ключи до получения указаний отправителя применять не разрешается.

4.12. При обнаружении бракованных криптографических ключей ключевой носитель с такими ключами следует вернуть изготовителю для установления причин происшедшего и их устранения в дальнейшем. Изготовитель в этом случае должен направить новые криптографические ключи.

4.13. Ключевые носители совместно с описью криптографических ключей должны храниться в сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и опись криптографических ключей совместно с другими документами, при этом ключевые

носители и опись криптографических ключей должны быть помещены в отдельную папку.

4.14. При отсутствии у пользователя СКЗИ сейфа (металлического шкафа) ключевые носители по окончании рабочего дня должны быть переданы ответственному пользователю средств СКЗИ по Журналу учёта СКЗИ.

5. Порядок эксплуатации СКЗИ и криптографических ключей к ним

5.1. Средства криптографической защиты информации эксплуатируются в Администрации в соответствии с правилами пользования ими, которые указаны в эксплуатационной и технической документации к СКЗИ.

5.2. СКЗИ и криптографические ключи используются в Администрации для обеспечения конфиденциальности и целостности электронных документов, в том числе при передаче информации по открытым каналам связи.

5.3. Конфиденциальность электронных документов обеспечивается путём их шифрования. Авторство и целостность электронных документов обеспечивается путём создания в документе электронной подписи пользователя.

5.4. Электронный документ может быть подписан электронной подписью с использованием только того закрытого ключа, для которого выдан сертификат ключа подписи пользователя с областью действия.

5.5. Для шифрования электронного документа пользователь использует свой собственный закрытый криптографический ключ и открытый криптографический ключ, соответствующий действующему закрытому криптографическому ключу получателя документа.

5.6. Открытый криптографический ключ содержится в сертификате ключа подписи, который выдаётся пользователю в электронной форме и на бумажном носителе.

5.7. Проверка подлинности электронной подписи электронного документа осуществляется пользователем с использованием открытого криптографического ключа отправителя документа.

5.8. Расшифровывание электронного документа осуществляется с использованием закрытого криптографического ключа пользователя и открытого криптографического ключа отправителя документа.

5.9. В случае необходимости генерации закрытого криптографического ключа (и пароля доступа к нему) пользователь должен осуществить генерацию самостоятельно на собственном АРМ (при наличии технической возможности[2])), либо на АРМ ответственного пользователя СКЗИ. При использовании ключевой информации рекомендуется в качестве носителей ключевой информации использовать носители, имеющие специализированные контейнеры ключевой информации, обеспечивающие невозможность их экспорта (также при генерации ключевой информации должен быть задан соответствующий параметр).

5.10. Пользователь не может подписать электронный документ своей электронной подписью или выполнить его шифрование, если истёк срок действия

---

2) В случае генерации пин-кода доступа администратором должна обеспечиваться смена пользователем пин-кода, при первом использовании носителю ключевой информации (обеспечивается функционалом носителя ключевой информации)

закрытых криптографических ключей. Также пользователь не может проверить электронную подпись электронного документа или произвести его расшифровывание в случае истечения срока действия сертификата ключа подписи, необходимого для выполнения соответствующей операции.

5.11. Реализованные в СКЗИ алгоритмы шифрования и электронной цифровой подписи гарантируют невозможность восстановления закрытых криптографических ключей отправителя по его открытым ключам.

5.12. При выявлении сбоев или отказов пользователь обязан сообщить о факте их возникновения ответственному пользователю СКЗИ и предоставить ему носители криптографических ключей для проверки их работоспособности. Проверку работоспособности носителей криптографических ключей администратор информационной безопасности выполняет в присутствии пользователя.

5.13. В случае если рабочие криптографические ключи потеряли работоспособность, то по заявке пользователя администратор информационной безопасности информации вскрывает конверт с резервными криптографическими ключами, делает копию ключевого носителя, используя резервные криптографические ключи, помещает резервные криптографические ключи в конверт.

5.14. В экстренных случаях, не терпящих отлагательства, вскрытие конверта с резервными криптографическими ключами может осуществляться пользователем самостоятельно с последующим уведомлением администратора информационной безопасности о факте вскрытия конверта с криптографическими ключами. На конверте делается запись о вскрытии с указанием даты и времени вскрытия конверта и подписью пользователя. Вскрытый конверт вместе с неработоспособными криптографическими ключами сдаются администратору информационной безопасности.

5.15. Вскрытие системного блока АРМ/сервера, на котором установлено СКЗИ, для проведения ремонта или технического обслуживания должно осуществляться в присутствии ответственного пользователя СКЗИ.

5.16. Пользователю запрещается:

осуществлять несанкционированное копирование криптографических ключей;

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

вставлять носители криптографических ключей в устройства считывания в режимах, не предусмотренных штатным режимом работы СКЗИ, а также в устройства считывания других автоматизированных рабочих мест и серверов;

записывать на носители с криптографическими ключами постороннюю информацию;

подключать к АРМ и серверам дополнительные устройства и соединители, не предусмотренные в комплектации;

вносить какие-либо изменения в программное обеспечение СКЗИ;

использовать бывшие в работе одноразовые ключевые носители для записи новых криптографических ключей.

6. Порядок действий при компрометации криптоключей

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

К компрометации ключей относятся следующие события:

утрата носителей ключа;

утрата носителей ключа с последующим обнаружением;

увольнение работников, имевших доступ к ключевой информации;

возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;

нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;

утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;

утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;

доступ посторонних лиц к ключевой информации;

другие события утери доверия к ключевой документации.

6.2. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать администратору информационной безопасности.

6.3. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, не предъявлении ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

6.4. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет обладатель скомпрометированной конфиденциальной информации. Действующие и резервные ключевые документы, предназначенные для применения в случае компрометации действующих криптоключей, должны храниться во внутреннем отсеке сейфа в различных конвертах.

6.5. Порядок действий пользователя при компрометации ключей:

Решение о факте или угрозе компрометации своего криптоключа пользователь принимает самостоятельно. При компрометации ключа пользователь должен прекратить работу с скомпрометированным ключам и оповестить администратора информационной безопасности. При наличии возможности оповестить пользователей, с которыми осуществлялось взаимодействие посредством скомпрометированных ключей.

6.6. Порядок действий при сообщении о компрометации криптоключей:

При получении сообщения о компрометации ключа пользователя, администратор информационной безопасности ответным звонком уточняет факт компрометации, и в случае его подтверждения немедленно приостанавливает

действие ключа. При наличии резервных ключей, пользователь должен перейти на комплект резервных ключей. Если резервные ключи не были предусмотрены, для восстановления системы необходимо: повторно произвести формирование ключа; обеспечить получение новых криптоключей пользователями системы.

7. Уничтожение средств криптографической защиты информации

7.1. Криптографические ключи:

7.1.1. Уничтожению подлежат криптографические ключи в случае их компрометации, вывода из эксплуатации, окончания срока действия.

7.1.2. Криптографические ключи уничтожаются путём их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования, в соответствии с требованиями эксплуатационной и технической документации на СКЗИ, путем удаления с носителя информации, способом, препятствующим восстановлению удаленной информации, или физическим уничтожением материального носителя ключевой информации.

7.2. Аппаратные СКЗИ:

7.2.1. Уничтожению подлежат аппаратные СКЗИ вышедшие из строя или выведенные из эксплуатации.

7.2.2. Аппаратные СКЗИ уничтожаются (утилизируются) в соответствии с требованиями Положения ПКЗ-2005, по решению обладателя конфиденциальной информации, владеющего СКЗИ, и по согласованию с ОКЗИ (специальным структурным подразделением).

7.3. Программные СКЗИ:

7.3.1. Уничтожению подлежат программные СКЗИ выведенные из эксплуатации.

7.3.2. Программные СКЗИ уничтожаются путем предусмотренным эксплуатационной и технической документацией к СКЗИ. В противном случае, удалением программного обеспечения СКЗИ с носителя информации, способом, препятствующим восстановлению удаленной информации.

7.4. Программно-аппаратные СКЗИ:

7.4.1. Уничтожению подлежат программно-аппаратные СКЗИ вышедшие из строя или выведенные из эксплуатации.

7.4.2. Намеченные к уничтожению (утилизации) СКЗИ, извлекаются из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ, процедура удаления программного обеспечения СКЗИ, и они полностью отсоединены от аппаратных средств.

7.5. Дистрибутивы СКЗИ:

7.5.1. Уничтожению подлежат дистрибутивы выведенных из эксплуатации СКЗИ, ПО СКЗИ и скомпрометированных ключевых дистрибутивов на носителях информации.

7.5.2. Дистрибутивы СКЗИ уничтожаются путем удаления с носителя информации, способом, препятствующим восстановлению удаленной информации, либо физическим уничтожением материального носителя.

7.6. Ключевые документы:

7.6.1. Уничтожению подлежат скомпрометированные или выведенные из эксплуатации ключевые документы.

7.6.2. Ключевые документы уничтожаются путем удаления с носителя ключевой информации, способом, препятствующим восстановлению удаленной информации, физическим уничтожением материального носителя ключевых документов, путем сжигания, с помощью любых бумагорезательных машин или иного физического воздействия, в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из эксплуатации (окончания срока действия).

7.7. Эксплуатационная и техническая документация к СКЗИ:

7.7.1. Эксплуатационная и техническая документация подлежит уничтожению вместе с поставляемым СКЗИ, выведенным из эксплуатации.

7.7.2. Эксплуатационная и техническая документация к СКЗИ уничтожается путем сжигания или с помощью любых бумагорезательных машин.

7.8. СКЗИ уничтожаются комиссией, состоящей из работников ОКЗИ (специального структурного подразделения), не менее двух представителей, и не менее двух работников Администрации.

7.8.1. При уничтожении СКЗИ комиссия обязана:

установить наличие оригинала и количество копий СКЗИ;

проверить внешним осмотром целостность каждого СКЗИ;

установить наличие на оригинале и всех копиях СКЗИ реквизитов путём сверки с записями в Журнале учёта СКЗИ;

убедиться, что СКЗИ действительно подлежат уничтожению;

произвести уничтожение СКЗИ;

составить акт об уничтожении СКЗИ.

7.9. Акт об уничтожении СКЗИ:

7.9.1. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров, уничтожаемых СКЗИ, эксплуатационной и технической документации СКЗИ.

7.9.2. В Журнале учёта СКЗИ ответственным пользователем СКЗИ производится отметка об уничтожении СКЗИ с указанием даты и номера Акта.

7.9.3. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении.

7.9.4. Акт об уничтожении СКЗИ подписывается председателем комиссии, членами комиссии.

7.9.5. Акты об уничтожении СКЗИ хранятся у ответственного пользователя СКЗИ.

7.9.6. Форма акта об уничтожении СКЗИ приведена в приложении 8 к настоящей политике.

8. Организация режима в помещениях, где установлены СКЗИ или хранятся криптографические ключи

8.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся криптографические ключи, должны обеспечивать сохранность СКЗИ и криптографических ключей.

8.2. При обустройстве данных помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

8.3. Спецпомещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решётками или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

8.4. Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также визуальное наблюдение посторонними лицами за проведением работ в помещении.

8.5. Режим охраны помещений, в том числе правила допуска работников и посетителей в рабочее и нерабочее время устанавливается главой муниципального образования Северский муниципальный район. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей политики.

8.6. Двери спецпомещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода работников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают работникам, имеющим право допуска в спецпомещения, под расписку в журнале учёта хранилищ СКЗИ и ключей от них (форма журнала учёта хранилищ СКЗИ и ключей от них приведена в приложении 9). Дубликаты ключей от входных дверей таких помещений следует хранить в специальном сейфе.

8.7. Окна помещений, в которых установлены СКЗИ должны быть защищены для предотвращения несанкционированного просмотра.

8.8. Помещения, по возможности, должны быть оснащены системой контроля и управления доступом, охранной сигнализацией, связанной со службой охраны здания или дежурным. Исправность сигнализации периодически должна проверяться службой охраны.

8.9. Для хранения криптографических ключей, эксплуатационной и технической документации, дистрибутивов СКЗИ должно быть предусмотрено необходимое число надёжных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей или кодовыми замками, или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у ответственного пользователя СКЗИ. Дубликаты ключей от хранилищ пользователи хранят в специальном сейфе. По окончании рабочего дня помещение и установленные в нём хранилища должны быть закрыты,

хранилища опечатаны. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей, ответственных за эти хранилища.

8.10. В обычных условиях помещения и находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями или администратором информационной безопасности.

8.11. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю СКЗИ, который должен оценить возможность компрометации хранящихся криптографических ключей, составить акт и принять при необходимости меры к локализации последствий компрометации криптографических ключей и к их замене.

8.12. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптографических ключей в присутствии лиц, не допущенных к работе с данными СКЗИ, не допускается.

8.13. На время отсутствия пользователей необходимое оборудование при наличии технической возможности должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с ответственным пользователем СКЗИ необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в отсутствие пользователя.

9. Порядок использования защищенных каналов связи

9.1. При использовании защищенного канала связи необходимо:

обеспечить информационную безопасность каждого информационного актива в соответствии с действующим законодательством Российской Федерации (АРМ, сервера, телекоммуникационного оборудования) подключаемого к защищенному каналу связи;

обеспечить в соответствии с настоящей политикой надлежащие условия для размещения и функционирования информационного актива, подключенного к защищенному каналу связи и исключить несанкционированный доступ в помещения, где расположены информационные активы;

для защиты информационного актива, участвующих в обмене информации, выходящих за пределы контролируемой зоны, должна проводиться периодическая проверка на отсутствие уязвимостей с использованием анализа защищенности;

обеспечить периодический контроль целостности неизменяемых файлов, используемых в программном обеспечении информационных активов;

обеспечить контроль изменения прикладной программной среды, исключение ввода в информационные активы программных средств без их предварительной гарантированной проверки;

обеспечить мероприятия по антивирусной защите, обеспечению свободной от вирусов программной среды информационных активов и от внешнего периметра сети.

9.2. При эксплуатации защищённого канала связи необходимо соблюдать следующие правила:

использовать защищенный канал связи только по прямому назначению;

не допускать использование защищенного канала связи в личных целях;

обеспечивать сохранность информационных ресурсов и физической целостности оборудования;

не допускать распространения спама и вредоносных компьютерных программ с АРМ Пользователя;

не допускать нарушений установленного настоящей политикой порядка эксплуатации СКЗИ и осуществления иных несанкционированных действий.

10. Ответственность за исполнение положений настоящей политики

10.1. Ответственность за исполнение положений настоящей политики возлагается на всех работников Администрации, осуществляющих работу со средствами криптографической защиты информации.

10.2. Пользователи СКЗИ Администрации обязаны:

соблюдать требования настоящей политики в отношении учёта, хранения и использования средств криптографической защиты информации;

не нарушать установленные правила доступа в помещения;

незамедлительно сообщать ответственному пользователю СКЗИ обо всех выявленных нарушениях обращения с СКЗИ или фактов доступа в помещения с нарушением установленных правил;

использовать криптографические средства защиты информации только в соответствии с эксплуатационной и технической документацией.

10.3. Ответственный пользователь СКЗИ обязан:

соблюдать требования настоящей политики в отношении учёта, хранения и использования средств криптографической защиты информации;

вести поэкземплярный учёт используемых СКЗИ, эксплуатационной и технической документации к ним

не нарушать установленные правила доступа в помещения;

участвовать в служебных проверках по факту нарушения требований настоящей политики;

осуществлять замену криптографических ключей из резервных в случаях компрометации или потери работоспособности ключевого носителя с основными криптографическими ключами;

в случае необходимости разъяснять пользователям средств криптографической защиты информации особенности и порядок работы с ними.

Лица, виновные в нарушении положений настоящей политики, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой и административной ответственности.

Начальник управления информатизации
и информационной безопасности Н.Н. Сергиевская

Приложение 1
к политике использования средств
криптографической защиты
администрации муниципального
образования Северский
муниципальный район
Краснодарского края

ФОРМА

Акт №__
установки и ввода в эксплуатацию
средства криптографической защиты информации

станица Северская « » _____ 20___г.

Настоящий акт составлен о том, что работником _____
(наименование организации)

(далее – Исполнитель) была произведена установка и настройка средства криптографической защиты информации _____ (далее - криптосредство) в Администрации.

Серийный номер (инвентарный номер) ПЭВМ / сервера: _____

Место установки: _____

ФИО ответственного работника СКЗИ:_____

ФИО пользователя ПЭВМ:_____

Учетный номер СКЗИ: _____

Серийный номер СКЗИ: _____

Регистрационный номер криптосредства (ПАК): _____

Регистрационный номер экземпляра ключевого документа: _____

Установленное и настроенное криптосредство находится в работоспособном состоянии.

Пользователь криптосредства обязуется:

не разглашать конфиденциальную информацию, к которой он допущен, в том числе сведения о криптоключах;

соблюдать требования к обеспечению безопасности криптосредств и ключевых документов к ним;

сдать криптосредство, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранения от исполнения обязанностей, связанных с использованием криптосредств;

сообщать исполнителю о попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

немедленно уведомлять исполнителя о фактах утраты или недостачи криптосредств, ключевых документов к ним.

Исполнитель

_____/_____/
подпись ФИО

Пользователь криптосредства

_____/_____/
подпись ФИО

Начальник управления информатизации
и информационной безопасности Н.Н.Сергиевская

Приложение 2
к политике использования средств
криптографической защиты
администрации муниципального
образования Северский
муниципальный район
Краснодарского края

ФОРМА

ПРОТОКОЛ № ___
принятия зачета у пользователя средств криптографической защиты информации администрации муниципального образования Северский муниципальный район

Зачет проведен в соответствии с Перечнем вопросов по проверке знаний у пользователей средств криптографической защиты информации, утвержденным руководителем ОКЗИ _____.
(наименование организации)

Результаты зачета приведены в таблице 1.
Таблица 1 – Результат сдачи зачета

№ п/п	Фамилия, имя, отчество пользователя	Номер билета	Зачет/ незачет	Подпись пользователя

Должность работника ОКЗИ _____/_____/
(подпись) (ФИО)

Начальник управления информатизации
и информационной безопасности Н.Н.Сергиевская

Приложение 3
к политике использования средств
криптографической защиты
администрации муниципального
образования Северский
муниципальный район
Краснодарского края

ФОРМА

Администрация муниципального образования Северский муниципальный район

ЛИЦЕВОЙ СЧЕТ
пользователя СКЗИ

_____

(ФИО)

_____

(отдел, должность)

Наименование СКЗИ	Серийные номера СКЗИ	Регистрационные номера экземпляров ключевых документов	Дата и расписка о получении СКЗИ	Дата и расписка возвращения СКЗИ	Примечания
1	2	3	4	5	6

Должность работника ОКЗИ _____/_____/
(подпись) (ФИО)

Начальник управления информатизации
и информационной безопасности Н.Н.Сергиевская

Приложение 4
к политике использования средств
криптографической защиты
администрации муниципального
образования Северский
муниципальный район
Краснодарского края

ФОРМА

УТВЕРЖДАЮ
Руководитель органа
криптографической защиты информации

_____
(Наименование организации)

_____ _____
(подпись) (Ф.И.О.)

«____» _____ 20__ года.

ЗАКЛЮЧЕНИЕ

о возможности допуска пользователей к самостоятельной работе со средствами криптографической защиты информации администрации муниципального образования Северский муниципальный район

Пользователи, получившие ключевой носитель, а также пользователи, назначенные приказом главы муниципального образования Северский муниципальный район, прошедшие обучение и сдавшие зачет по использованию СКЗИ, допущены к самостоятельной работе и обязуется:

не разглашать конфиденциальную информацию, к которой допущен, в том числе сведения о криптоключах;

соблюдать требования к обеспечению безопасности хранения, обработки и передачи конфиденциальной информации по каналам связи с использованием СКЗИ;

сообщать оператору о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

сдать установленным порядком СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

немедленно уведомлять оператора о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ (сейфов), личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Перечень лиц, прошедших обучение и сдавших зачет по средства криптографической, представлен в таблице 1.

Таблица 1 – Список пользователей СКЗИ

№ п/п	Должность	ФИО	Наименование криптосредства

Должность работника ОКЗИ _____/_____/
(подпись) (ФИО)

Начальник управления информатизации
и информационной безопасности Н.Н.Сергиевская

Приложение 5
к политике использования средств
криптографической защиты
администрации муниципального
образования Северский
муниципальный район
Краснодарского края

ФОРМА

Технический (аппаратный) журнал

№ п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			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

Начальник управления информатизации
и информационной безопасности Н.Н.Сергиевская

Приложение 6
к политике использования средств
криптографической защиты
администрации муниципального
образования Северский
муниципальный район
Краснодарского края

ФОРМА

АКТ №__
уничтожения СКЗИ
администрации муниципального образования Северский муниципальный район

Состав комиссии:

Председатель комиссии _____ _____

Члены комиссии _____ _____

_____ _____

Комиссия произвела отбор к уничтожению ключевых документов:

№ п/п	Тип и регистрационный номер СКЗИ	Тип ключевого документа	Серийный номер и номер экземпляра ключевого документа	Номер носителя ключевого документа	Дата регистрации
1	2	3	4	5	6

Всего подлежит уничтожению _____(_____)
наименований документов (цифрами) (прописью)

Ключевые документы уничтожены гарантированным стиранием ключевой информации с ключевого носителя.

Председатель комиссии _____ _____

Члены комиссии _____ _____

_____ _____

Начальник управления информатизации
и информационной безопасности Н.Н.Сергиевская

Приложение 7
к политике использования средств
криптографической защиты
администрации муниципального
образования Северский
муниципальный район
Краснодарского края

ФОРМА

ЖУРНАЛ УЧЁТА

хранилищ СКЗИ и ключей от них

Регистрационный номер	Наименование хранилища (сейф, металлический шкаф, кладовая, спец. хранилище)	Заводской, инвентарный номер хранилища	Местонахождение хранилища (подразделение, номер комнаты, корпуса, здания)	Что хранится (СКЗИ, ключевые документы, документация на СКЗИ)	Фамилия ответственного за хранилище	Количество комплектов ключей и их номера	Расписка ответственного за хранилище в получении ключа и дата	Расписка в обратном приёме ключа и дата	Примечание
1	2	3	4	5	6	7	8	9	10

Начальник управления информатизации
и информационной безопасности Н.Н.Сергиевская

Приложение 8
к политике использования средств
криптографической защиты
администрации муниципального
образования Северский
муниципальный район
Краснодарского края

ФОРМА

ЖУРНАЛ

поэкземплярного учёта СКЗИ, эксплуатационной и технической документации к ним, ключевых документов
(для обладателя конфиденциальной информации)

№ 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 СКЗИ		Отметка о выдаче СКЗИ		Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. работников органа криптографической защиты, пользователя СКЗИ, произведших подключение установку	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера, аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. работников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Начальник управления информатизации
и информационной безопасности Н.Н.Сергиевская