СОГЛАСОВАНО
Начальника Управления
защиты информации и специальной
документальной связи Аппарата
Губернатора Ханты-Мансийского
автономного округа – Югры

_____ А.Ю.Чиликов

ноября 2016г.

УТВЕРЖДАЮ
Заместитель Руководителя
Аппарата Губернатора
Ханты-Мансийского
автономного округа – Югры

_____ М.А.Киселев

ноября 2016г.

ПОЛОЖЕНИЕ
об организации криптографической защиты информации в Аппарате Губернатора Ханты-Мансийского автономного округа – Югры

СОСТАВИЛ
Заместитель начальника Управления –
начальник отдела технической защиты
информации и противодействия иностранным
технически разведкам Управления защиты информации и
специальной документальной связи
Аппарата Губернатора Ханты-Мансийского
автономного округа – Югры

_____ Тумаев М.А.

01 ноября 2016г.

1. Общие положения.

1.1. Настоящий документ разработан Управлением специальных мероприятий Аппарата Губернатора Ханты-Мансийского автономного округа – Югры в рамках, возложенных на него полномочий, определенных Положением об Управлении защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа – Югры, утвержденного распоряжением Аппарата Губернатора Ханты-Мансийского автономного округа – Югры от 03.02.2016 № 16-р.

1.2. Положение определяет порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных средств криптографической защиты (шифровальных средств) (далее – СКЗИ) подлежащей в соответствии с законодательством Российской Федерации обязательной защите информации с ограниченным доступом (в том числе персональных данных), не содержащей сведений, составляющих государственную тайну в Аппарате Губернатора Ханты-Мансийского автономного округа – Югры (далее – Аппарат Губернатора Югры).

1.3. Настоящее Положение не регламентирует порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ сведений, составляющих государственную тайну.

1.4. Настоящее Положение разработано в соответствии с требованиями:

Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

приказа ФАПСИ от 13 июня 2001 года № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

приказа ФСБ России от 09 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»

приказа ФСБ России от 21 февраля 2008 г. N 149/54-144 «Об утверждении методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»;

приказа ФСБ России от 21 февраля 2008 г. N 149/6/6-622 «Об утверждении 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.

1.5. Термины и определения, используемые в настоящем Положении:

средства шифрования - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;

средства имитозащиты - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации;

средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации функций создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи;

средства кодирования - средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций;

средства изготовления ключевых документов - аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств;

ключевые документы - электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах;

аппаратные шифровальные (криптографические) средства - устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с

алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин;

программные шифровальные (криптографические) средства - программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств;

программно-аппаратные шифровальные (криптографические) средства - устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.

1.6. Лица, допущенные к работе с СКЗИ:

ответственный за руководство работами по криптографической защите информации в Аппарате Губернатора Югры – начальник Управления защиты информации и специальной документальной связи Аппарата Губернатора Югры (далее – ответственный за руководство работами по КЗИ);

- ответственный за организацию и непосредственное выполнение мероприятий по криптографической защите информации в Аппарате Губернатора Югры – заместитель начальника отдела технической защиты информации и противодействия иностранным техническим разведкам (далее – Отдел ТЗИ и ПД ИТР) Управления защиты информации и специальной документальной связи (далее – Управление ЗИ и СДС), являющейся администратор информационной безопасности в соответствии с распоряжением Аппарата Губернатора от 25.01.2016 № 12-р «О назначении администратора информационной безопасности» (далее – ответственный за организацию работ по КЗИ);

пользователь СКЗИ – работник структурного подразделения Аппарата Губернатора Югры, допущенный к работе с СКЗИ в установленном порядке.

1.7. Допуск работников в Аппарате Губернатора Югры к работе с СКЗИ осуществляется в соответствии со списком лиц, допущенных к работе с СКЗИ, утвержденного ответственным за руководство работами по КЗИ в Аппарате Губернатора автономного округа (приложение 1).

1.8. Допуск работников Аппарата Губернатора Югры к работе с СКЗИ должен осуществляться после проведения ответственным за организацию работ по КЗИ обучения и ознакомления с требования по работе с СКЗИ. Факт

проведения обучения фиксируется в «Журнале учета инструктажа и обучения» (приложение 2).

1.9. Ответственный за организацию работ по КЗИ осуществляет учет используемых СКЗИ, технической и эксплуатационной документации к ним в «Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов» (приложение 2) и «Журнале технического (аппаратного) журнала» (приложение 3).

1.10. Контроль выполнения требований по эксплуатации СКЗИ осуществляет ответственный за организацию работ по КЗИ.

1.11. При выявлении фактов нарушения требований по эксплуатации СКЗИ Управлением ЗИ и СДС проводится разбирательство.

2. Порядок обращения с СКЗИ и криптоключами к ним

2.1. Предназначенные для обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации СКЗИ, а также ключевые документы к ним не должны содержать сведений, составляющих государственную тайну.

2.2. При необходимости передачи по техническим каналам связи служебных сообщений, касающихся организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, соответствующие указания необходимо передавать, только применяя СКЗИ.

2.3. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

2.4. Используемые и хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету по установленным формам в соответствии с требованиями Положения ПКЗ-2005. При этом программные СКЗИ должны учитывать 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.

Единицей поэкземплярного учета ключевых документов является ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведет ответственный за организацию криптографической защиты информации.

2.5. Все полученные обладателем конфиденциальной информации экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации пользователям СКЗИ, несущих персональную ответственность за их сохранность.

Ответственный за организацию работы по КЗИ вместо ведения лицевых счетов, ведет учет числящихся за пользователями СКЗИ, эксплуатационной и технической документации в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним.

2.6. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ под расписку в соответствующем журнале поэкземплярного учета. Такая передача между пользователями СКЗИ должна быть санкционирована ответственным за организацию криптографической защиты информации.

Обладатель конфиденциальной информации с согласия ответственного за организацию криптографической защиты информации может разрешить передачу СКЗИ, документации к ним, ключевых документов между допущенными к СКЗИ лицами по актам (составляется в свободной форме) без обязательной отметки в журнале поэкземплярного учета.

2.7. Пользователи СКЗИ хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей.

2.8. СКЗИ и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными нарочными из числа пользователей СКЗИ или ответственного за организацию криптографической защиты информации, для которых они предназначены, при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

Эксплуатационную и техническую документацию к СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

2.9. Для пересылки СКЗИ должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. СКЗИ пересылают отдельно от ключевых документов к ним. На упаковках указывают ответственного за организацию криптографической защиты информации или пользователя СКЗИ, для которых эти упаковки предназначены. На упаковках для пользователя СКЗИ делают пометку

«Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

Оформленную таким образом упаковку, при предъявлении фельдсвязью дополнительных требований, помещают во внешнюю упаковку, оформленную согласно предъявляемым требованиям. До первоначальной высылки (или возвращения) адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.

2.10. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо, в котором необходимо указать, что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления.

Сопроводительное письмо вкладывают в одну из упаковок.

2.11. Полученные упаковки вскрывают только в присутствии ответственного за организацию криптографической защиты информации или лично пользователи СКЗИ, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт (составляется в свободной форме), который высылает отправителю, а при необходимости информирует об этом ответственного за организацию криптографической защиты информации. Полученные с такими отправлениями СКЗИ и ключевые документы до получения указаний от отправителя и ответственного за организацию криптографической защиты информации применять не разрешается.

2.12. При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю через ответственного за организацию криптографической защиты информации для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от ответственного за организацию криптографической защиты информации или изготовителя.

2.13. Получение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме. Отправитель обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

2.14. Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов следует производить заблаговременно. Указание о вводе в действие очередных ключевых документов может быть дано только после поступления ответственному за организацию криптографической защиты информации подтверждения от всех заинтересованных пользователей СКЗИ о получении ими очередных ключевых документов.

2.15. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному за организацию криптографической защиты информации или по его указанию должны быть уничтожены на месте.

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

Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

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

2.17. СКЗИ уничтожают (утилизируют) в соответствии с требованиями Положения ПКЗ-2005 по решению обладателя конфиденциальной информации, владеющего СКЗИ.

Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию 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.

2.18. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

2.19. Ключевые документы должны быть уничтожены 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 действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

2.20. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в СКЗИ или иных дополнительных устройствах уничтожаются пользователями этих СКЗИ самостоятельно под расписку в техническом (аппаратном) журнале.

Ключевые документы уничтожаются либо пользователями СКЗИ, либо ответственным за организацию криптографической защиты информации под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом (составляется в свободной форме). При этом пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи СКЗИ должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) ответственного за организацию криптографической защиты информации для списания уничтоженных документов с их лицевых счетов (в случае их ведения). Не реже одного раза в год пользователи СКЗИ должны направлять ответственному за организацию криптографической защиты информации письменные отчеты об уничтоженных ключевых документах. Ответственный за организацию криптографической защиты информации

вправе устанавливать периодичность представления указанных отчетов чаще одного раза в год.

Уничтожение по акту производит комиссия в составе не менее двух человек – ответственного за организацию криптографической защиты информации и пользователя СКЗИ. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учета.

2.21. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. О выводе криптоключей из действия сообщают ответственному за организацию криптографической защиты информации. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственного за организацию криптографической защиты информации, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а передаваемая информация как можно менее ценной.

2.22. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать ответственному за организацию криптографической защиты информации. 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, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

2.23. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет обладатель скомпрометированной конфиденциальной информации.

2.24. Охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним установлены распоряжением Аппарата Губернатора Ханты-Мансийского автономного округа – Югры от 30.12.2010 № 281-р «Об Инструкции о пропускном и внутриобъектовом

режимах здания Дома Правительства Ханты-Мансийского автономного округа – Югры».

3. Порядок работа с СКЗИ

3.1. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам.

3.2. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

3.3. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

3.4. Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых носителей, создать рабочие копии. Копии должны быть соответствующим образом маркированы и должны использоваться, учитываться и храниться так же, как оригиналы.

3.5. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ под расписку в соответствующих журналах поэкземплярного учета.

Такая передача между пользователями СКЗИ должна быть санкционирована ответственным за организацию работ по КЗИ с согласия ответственного за руководство работами по КЗИ.

3.6. При обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов, нарушающих работу указанных средств, работа со СКЗИ на данном рабочем месте должна быть прекращена и организуются мероприятия по анализу и ликвидации негативных последствий данного нарушения.

4. Уровень криптографической защиты в Аппарате Губернатора автономного округа

Различаются шесть уровней криптографической защиты персональных данных (КС1, КС2, КС3, КВ1, КВ2, КА1), не содержащих сведений, составляющих государственную тайну, определенных в порядке возрастания количества и жесткости предъявляемых к криптосредствам требований, и,

соответственно, шесть классов криптосредств, также обозначаемых через КС1, КС2, КС3, КВ1, КВ2, КА1.

Уровень криптографической защиты персональных данных, обеспечиваемой криптосредством, определяется оператором путем отнесения нарушителя, действиям которого должно противостоять криптосредство, к конкретному типу.

При отнесении нарушителя к типу Н1 криптосредство должно обеспечить криптографическую защиту по уровню КС1, к типу Н2 - КС2, к типу Н3 - КС3, к типу Н4 - КС4, к типу Н5 - КС5, к типу Н6 - КС6.

Встраивание криптосредств класса КС1 и КС2 осуществляется без контроля со стороны ФСБ России (если этот контроль не предусмотрен техническим заданием на разработку (модернизацию) информационной системы).

Встраивание криптосредств класса КС3, КВ1, КВ2 и КА1 осуществляется только под контролем со стороны ФСБ России.

Встраивание криптосредств класса КС1, КС2 или КС3 может осуществляться либо самим пользователем криптосредства при наличии соответствующей лицензии ФСБ России, либо организацией, имеющей соответствующую лицензию ФСБ России.

Встраивание криптосредства класса КВ1, КВ2 или КА1 осуществляется организацией, имеющей соответствующую лицензию ФСБ России.

Поскольку для ИС Аппарата Губернатора Югры установлен тип нарушителя **Н1**, необходимо встраивание в ИС криптосредств класса **КС1**.

5. Действия в случае компрометации ключей

5.1. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать ответственному за организацию работ по КЗИ.

5.2. К компрометации ключей относятся следующие события:

утрата носителей ключа;

утрата иных носителей ключа с последующим обнаружением;

увольнение сотрудников, имевших доступ к ключевой информации;

возникновение подозрений на утечку информации или ее искажение;

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.

5.3. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия.

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

5.5. Мероприятия по розыску и локализации последствий компрометации информации ограниченного доступа, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет Управление ЗИ и СДС.

6. Изменения настоящего Положения

Настоящее Положение может быть дополнено либо изменено в связи с изменением требований законодательства Российской Федерации в сфере персональных данных. В случае внесения в настоящее Положение изменений, к ним будет обеспечен неограниченный доступ всем заинтересованным субъектам персональных данных.

Настоящее Положение действует до момента придания Аппарату Губернатора Ханты-Мансийского автономного округа – Югры статуса юридического лица и принятия в части обработки ПДн соответствующего распорядительного документа.

Приложение 1 к
положение об организации
криптографической защиты информации

ФОРМА

Утверждаю
Начальник Управления
защиты информации и специальной
документальной связи Аппарата
Губернатора Ханты-Мансийского
автономного округа – Югры
_____ФИО
«_____» _____ 20____г.

Перечень пользователей СКЗИ Аппарата Губернатора Ханты-Мансийского автономного округа – Югры

№ п/п	Фамилия Имя Отчество	Должность	Назначение СКЗИ *(для работы в ГИС, бухгалтерских системах или государственных сайтах)*	Наименование СКЗИ *(ViPNet Client, КриптоПро, электронная подпись)*	От кого получены СКЗИ

Подготовил:
Заместитель начальника отдела технической защиты информации и
противодействия иностранным техническим разведкам
Управления защиты информации и специальной документальной связи Аппарата
Губернатора Ханты-Мансийского автономного округа – Югры
_____ФИО
«_____» _____ 20____г.

Приложение 2 к
положение об организации
криптографической защиты информации

ФОРМА

Типовая форма
журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

N п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников 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. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение 3 к
положение об организации
криптографической защиты информации

ФОРМА

Типовая форма технического (аппаратного) журнала

N 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 криптоключи	Дата	Подпись Пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10