Министерство социальной политики и труда Удмуртской Республики
(Минсоцполитики УР)

Удмурт Элькунысь мерлыко политикая но ужъя министерство
(УЭ мерполитикмин)

ПРИКАЗ

«09» февраля 2018 г. № 87

г. Ижевск

Об утверждении Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», 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 защищенности», приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации 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» п р и к а з ы в а ю:

1. Утвердить прилагаемую Инструкцию по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики.

2. Признать утратившими силу:

приказ Министерства социальной, семейной и демографической политики Удмуртской Республики от 2 июня 2016 года № 120 «Об утверждении Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной, семейной и демографической политики Удмуртской Республики»;

приказ Министерства социальной, семейной и демографической политики Удмуртской Республики от 30 декабря 2016 года № 242 «О внесении

изменения в приказ Министерства социальной, семейной и демографической политики Удмуртской Республики от 2 июня 2016 года № 120 «Об утверждении Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной, семейной и демографической политики Удмуртской Республики».

3. Контроль за исполнением настоящего приказа возложить на заместителя министра Белоусову М.Е.

Министр Т.Ю. Чуракова

УТВЕРЖДЕНА
приказом Министерства
социальной политики и труда
Удмуртской Республики
от «09» 02 2018 года № 87

ИНСТРУКЦИЯ
по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

I. Общие положения

1. Настоящая Инструкция определяет порядок учёта, хранения и использования средств криптографической защиты информации и криптографических ключей для защиты персональных данных, а также порядок изготовления, смены, уничтожения средств криптографической защиты информации и действий сотрудников Министерства социальной политики и труда Удмуртской Республики (далее – Министерство) при компрометации криптографических ключей в целях обеспечения безопасности эксплуатации средств криптографической защиты информации.

2. Инструкция разработана в соответствии с требованиями:

Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

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, утверждённых приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378;

Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утверждённого приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66;

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, утверждённой

приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152;

Требований к защите персональных данных при их обработке в информационных системах персональных данных, утверждённых постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119.

3. В настоящей Инструкции используются следующие основные понятия:

автоматизированное рабочее место (далее – АРМ) – комплекс оборудования, вычислительная машина, предназначенные для эксплуатации пользователем средств криптографической защиты информации в рамках исполнения должностных обязанностей;

ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее – проверка электронной подписи);

ключевая информация – специальным образом организованная совокупность криптографических ключей, предназначенная для осуществления криптографической защиты информации в течение определённого срока;

ключевой материал – совокупность всех криптографических ключей участников криптографической системы и информация, сопровождающая их применение в средств криптографической защиты информации;

ключевой носитель – физический носитель определённой структуры, предназначенный для размещения на нём ключевой информации (исходной ключевой информации); различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования (магнитная лента, дискета, компакт - диск, Data Key, Smart Card, Touch Memory и т.п.);

компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптографическими ключами и ключевыми носителями, в результате которых криптографические ключи могут стать доступными несанкционированным лицам и (или) процессам;

конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

криптографический ключ – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

опечатывающее устройство – устройство, предназначенное для опечатывания дверей помещений, сейфов, металлических шкафов от несанкционированного вскрытия и применяемое совместно с пломбиром;

персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных);

пользователь средств криптографической защиты информации – уполномоченное должностное лицо, допущенное к работе со средствами криптографической защиты информации, участвующее в эксплуатации средств криптографической защиты информации или использующее результаты его функционирования, ответственное за обеспечение безопасности средств криптографической защиты информации при хранении, обработке и передаче информации по каналам связи с использованием средств криптографической защиты информации;

помещение для хранения средств криптографической защиты информации – помещение в здании Министерства, выделенное для хранения дистрибутивов используемых средств криптографической защиты информации, эксплуатационно-технической документации на средства криптографической защиты информации, ключевых носителей и (или) криптографических ключей;

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;

средства криптографической защиты информации (далее – СКЗИ) – совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования и защиты от несанкционированного доступа информации, не содержащей сведений, составляющих государственную тайну, при её передаче по каналам связи, обработке и хранении.

К СКЗИ относятся:

а) средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при её обработке и хранении;

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

в) средства электронной подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций:

создание электронной подписи с использованием закрытой части криптографического ключа электронной подписи;

подтверждение подлинности электронной подписи с использованием открытой части криптографического ключа электронной подписи;

создание закрытой и открытой частей криптографического ключа электронной подписи;

г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путём ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых носителей (независимо от вида носителя ключевой информации);

е) ключевые носители (независимо от вида носителя ключевой информации);

удостоверяющий центр – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

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.

II. Организация криптографической защиты информации в Министерстве

4. Министерство использует сертифицированные Федеральной службой безопасности Российской Федерации СКЗИ, предназначенные для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну и персональных данных, обрабатываемых в Министерстве.

5. Все действия с СКЗИ осуществляются в соответствии с эксплуатационно-технической документацией на СКЗИ.

6. Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управлению криптографическими ключами приказом Министерства назначается администратор безопасности за эксплуатацию СКЗИ.

7. Администратор безопасности за эксплуатацию СКЗИ обязан обладать знаниями в области организации криптографической защиты, а также иметь необходимый уровень квалификации по обеспечению безопасности хранения, обработки и передачи информации ограниченного доступа с использованием СКЗИ.

8. Администратор безопасности за эксплуатацию СКЗИ в процессе осуществления работ по криптографической защите информации в

Министерстве выполняет следующие обязанности:

1) осуществляет организацию и обеспечение бесперебойной работы СКЗИ;

2) разрабатывает правила работы с СКЗИ;

3) осуществляет подготовку к эксплуатации СКЗИ (заполнение формуляров, печать эксплуатационно-технической документации на СКЗИ);

4) ведёт поэкземплярный учёт СКЗИ, эксплуатационно-технической документации на СКЗИ и дистрибутивов используемых СКЗИ;

5) хранит и выдаёт СКЗИ, эксплуатационно-техническую документацию на СКЗИ;

6) устанавливает программное обеспечение VipNet Client на АРМ с составлением Акта ввода в эксплуатацию средств криптографической защиты информации (ПО VipNet Client) по форме согласно приложению 1;

7) устанавливает СКЗИ на АРМ с составлением Акта ввода в эксплуатацию средств криптографической защиты информации по форме согласно приложению 2;

8) выполняет настройки СКЗИ и средств защиты от несанкционированного доступа (далее – НСД);

9) ведёт учёт пользователей СКЗИ с регистрацией в Журнале учёта пользователей средств криптографической защиты информации по форме согласно приложению 3 и принимает зачёт на допуск к самостоятельной работе с СКЗИ у пользователей СКЗИ;

10) проводит инструктаж пользователей СКЗИ не реже одного раза в год с отметкой в Журнале инструктажа пользователей информационных систем персональных данных (ИСПДн) по форме согласно приложению 4;

11) контролирует работоспособность СКЗИ;

12) осуществляет отслеживание сроков действия сертификатов соответствия на СКЗИ;

13) производит изъятие СКЗИ в случае увольнения или отстранения от исполнения обязанностей пользователя, связанных с использованием СКЗИ, по форме согласно приложению Приложение 5;

14) осуществляет уничтожение СКЗИ, эксплуатационно-технической документации на СКЗИ в случае окончания срока действия сертификата соответствия на СКЗИ или лицензионного соглашения с составлением Акта о списании и уничтожении средств криптографической защиты информации по форме согласно приложению 6;

15) проводит расследование и составление заключений по фактам нарушений условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;

16) осуществляет разработку и принятие мер по предотвращению возможных негативных последствий нарушения условий использования СКЗИ;

17) оказывает консультативную и методическую помощь пользователям СКЗИ в использовании и обеспечении функционирования СКЗИ при обработке защищаемой информации;

18) осуществляет контроль за соблюдением условий использования, функционирования и хранения ключевых материалов и СКЗИ в соответствии с эксплуатационно-технической документацией на СКЗИ и настоящей Инструкцией;

19) осуществляет подготовку к эксплуатации криптографических ключей (оформление бланков заявлений и доверенностей, взаимодействие с удостоверяющими центрами);

20) выполняет копирование криптографических ключей на резервные носители;

21) ведёт поэкземплярный учёт, хранение и выдачу криптографических ключей;

22) устанавливает криптографические ключи на АРМ пользователя СКЗИ;

23) осуществляет уничтожение криптографических ключей по истечении срока действия или компрометации криптографических ключей с составлением Акта о списании и уничтожении ключевых материалов по форме согласно приложению 7;

24) ведёт поэкземплярный учёт, выдачу и приём опечатывающих устройств в Журнале учёта опечатывающих устройств по форме согласно приложению 8;

25) обеспечивает организацию режима конфиденциальности в отношении паролей доступа;

26) осуществляет контроль настроек на АРМ пользователей СКЗИ;

27) проводит не реже 1 раза в год проверки АРМ пользователей СКЗИ с отметкой в Журнале проверки установленных средств криптографической защиты информации на автоматизированном рабочем месте по форме согласно приложению 9.

9. Администратор безопасности за эксплуатацию СКЗИ вправе поручить государственным гражданским служащим управления информационных ресурсов выполнение обязанностей, предусмотренных подпунктами 3 - 9, 12 - 14,15, 17 - 22 пункта 8 настоящей Инструкции (далее – сотрудник, на которого возложены обязанности по организации криптографической защиты информации).

10. Сотрудник, на которого возложены обязанности по организации криптографической защиты информации, должен обладать знаниями в области организации криптографической защиты информации, а также иметь необходимый уровень квалификации по обеспечению безопасности хранения, обработки и передачи информации ограниченного доступа с использованием СКЗИ.

11. Администратор безопасности за эксплуатацию СКЗИ при осуществлении контроля настроек на АРМ пользователей СКЗИ обеспечивает соблюдение следующих требований:

1) исключение возможности загрузки и использования нестандартных, изменённых или отладочных версий операционных систем;

2) исключение возможности удалённого управления, администрирования и модификации операционной системы и её настроек;

3) отключение всех неиспользуемых ресурсов системы (протоколы, сервисы и т.п.);

4) настройка на максимальный уровень режимов безопасности, реализованных в операционной системе;

5) обеспечение мер, максимально ограничивающих доступ к ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части), системному реестру, журналам системы, файлам подкачки, кэшируемой информации (пароли и т.п.), отладочной информации;

6) исключение попадания в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;

7) установка пакетов обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.) и антивирусных баз;

8) активирование подсистемы регистрации событий информационной безопасности;

9) включения автоматической блокировки экрана после ухода пользователя СКЗИ с рабочего места.

12. Администратор безопасности за эксплуатацию СКЗИ либо сотрудник, на которого возложены обязанности по организации криптографической защиты информации (далее – уполномоченное лицо) осуществляют работы по криптографической защите информации в Министерстве.

13. Допуск пользователей СКЗИ к работе с СКЗИ в Министерстве оформляется приказом Министерства.

14. Пользователь СКЗИ обязан:

1) соблюдать требования к обеспечению безопасности персональных данных, СКЗИ и криптографических ключей;

2) проходить подготовку с последующим допуском к самостоятельной работе с СКЗИ в соответствии с должностными обязанностями;

3) хранить ключевые носители с криптографическими ключами в сейфе, в условиях, исключающих бесконтрольный доступ к ним, а также их искажение или несанкционированное уничтожение;

4) соблюдать требования эксплуатационно-технической документации на СКЗИ;

5) хранить в нерабочее время, в случае временного отсутствия на работе (болезнь, командировка, отпуск) ключевые носители с криптографическими ключами в запираемом на замок и опечатанном металлическом шкафу или сейфе (далее – сейф), либо сдавать на хранение администратору безопасности за эксплуатацию СКЗИ;

6) сдавать ключевые носители с криптографическими ключами при замене АРМ с установленным СКЗИ, при переустановке программного обеспечения. При этом на АРМ должно быть деинсталлировано программное обеспечение СКЗИ;

7) сдавать СКЗИ, ключевые носители с криптографическими ключами с документальным оформлением в соответствии с порядком, установленным настоящей Инструкцией при прекращении использования СКЗИ (увольнение, перевод на другую работу, не связанную с использованием СКЗИ) ;

8) опечатывать сейф и помещение личным средством опечатывания (далее – пломбир) или ярлыками по окончании рабочего дня;

9) уведомлять незамедлительно администратора безопасности за эксплуатацию СКЗИ о фактах получения сведений об используемых СКЗИ посторонними лицами, утраты или недостачи СКЗИ, криптографических ключей, ключей от помещений, сейфов и других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений;

10) прекратить работу с СКЗИ на своем рабочем месте, при обнаружении на АРМ, оборудованном СКЗИ, посторонних программ или вирусов; проинформировать о факте установки посторонних программ или вирусов администратора безопасности за эксплуатацию СКЗИ, который организует мероприятия по анализу и ликвидации негативных последствий данного нарушения.

15. Пользователю СКЗИ запрещается:

1) разглашать закрытую ключевую информацию и другую информацию ограниченного доступа, передавать другим лицам СКЗИ, носители ключевой информации и пароли, выводить закрытую ключевую информацию на монитор и принтер;

2) вносить какие-либо несанкционированные изменения в СКЗИ и аппаратно-программные средства, работающие совместно с установленными СКЗИ и способными влиять на функционирование СКЗИ;

3) изменять настройки СКЗИ;

4) осуществлять вскрытие системных блоков АРМ с установленными СКЗИ, подключать к ним дополнительные устройства и соединители, не предусмотренные штатной комплектацией;

5) оставлять без контроля ключевые носители, а также АРМ с установленными СКЗИ при включенном питании;

6) допускать просмотр на мониторе информации ограниченного доступа, обрабатываемой с использованием СКЗИ, в присутствии лиц, не имеющих к этой информации непосредственного отношения;

7) хранить закрытые ключи электронной подписи и шифрования в памяти АРМ в незашифрованном виде;

8) выносить ключевые носители за пределы служебных помещений без разрешения;

9) применять скомпрометированные криптографические ключи;

10) осуществлять несанкционированное копирование ключевой информации на неучтённый ключевой носитель;

11) вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным порядком использования ключевого носителя;

12) записывать на ключевые носители какую-либо информацию, не предусмотренную правилами пользования на СКЗИ;

13) устанавливать носители с личной ключевой информацией на АРМ других пользователей;

14) производить записи новых криптографических ключей на машинные носители ключевой информации без предварительного уничтожения ранее записанной ключевой информации, если иной порядок не определён эксплуатационно-технической документацией на СКЗИ;

15) работать на технических средствах при обнаружении факта несанкционированного вскрытия системного блока АРМ, наличия «посторонних» (незарегистрированных) программ, нарушения целостности программного обеспечения; по данному факту организуется служебное расследование и проводятся работы по анализу и ликвидации негативных последствий нарушения;

16) устанавливать на АРМ нелицензионное программное обеспечение для предупреждения возможности занесения вирусов и других вредоносных программ.

III. Учёт и хранение СКЗИ, эксплуатационно-технической документации на СКЗИ и криптографических ключей

16. СКЗИ, эксплуатационно-техническая документация на СКЗИ, криптографические ключи, и дистрибутивы используемых СКЗИ, используемые для обеспечения безопасности персональных данных, подлежат поэкземплярному учёту и хранению в сейфах.

17. Поэкземплярный учёт СКЗИ ведётся в Журнале поэкземплярного учёта средств криптографической защиты информации, эксплуатационно-технической документации к ним (далее – журнал учёта СКЗИ) по форме согласно приложению 10. 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 также учитываются совместно с соответствующими аппаратными средствами.

18. Единицей поэкземплярного учёта криптографических ключей считается отчуждаемый ключевой носитель многократного использования.

19. Пользователь СКЗИ может одновременно иметь несколько криптографических ключей и соответствующих им сертификатов ключей проверки электронной подписи.

20. Поэкземплярный учёт криптографических ключей ведётся в Журнале поэкземплярного учёта ключевых материалов (далее – журнал учёта ключей) по форме согласно приложению 11. Если один и тот же ключевой носитель многократно используется для записи криптографических ключей, то носитель каждый раз регистрируется вновь.

21. Все полученные экземпляры СКЗИ должны быть выданы под роспись в журнале учёта СКЗИ пользователю СКЗИ, который несёт персональную ответственность за их сохранность.

22. При необходимости пользователю СКЗИ выдаётся эксплуатационно-техническая документация на СКЗИ с последующим её возвратом.

23. Дистрибутивы используемых СКЗИ, эксплуатационно-техническая документация на СКЗИ и инструкции хранятся в помещении для хранения СКЗИ.

24. Уполномоченное лицо выдаёт пользователю СКЗИ криптографические ключи (рабочие и резервные) под роспись в журнале учёта ключей. Пользователь СКЗИ несёт персональную ответственность за сохранность выданных ему криптографических ключей.

25. Пользователь СКЗИ использует резервные криптографические ключи в случае неработоспособности рабочих криптографических ключей.

26. Уполномоченное лицо и пользователь СКЗИ хранят криптографические ключи в сейфах.

27. При отсутствии у пользователя СКЗИ сейфа в начале рабочего дня пользователь СКЗИ должен получить у уполномоченного лица ключевые носители в опечатанном конверте, а в конце рабочего дня сдать их с отметкой в Журнале учёта и выдачи средств криптографической защиты информации, ключевых материалов, ключей от сейфов и металлических шкафов по форме согласно приложению 12.

28. Уполномоченное лицо принимает ключевые носители с неработоспособными криптографическими ключами от пользователя СКЗИ. Неработоспособные ключевые носители подлежат уничтожению путём физического уничтожения ключевого носителя или путём переформатирования ключевых носителей средствами программного обеспечения СКЗИ по технологии, принятой для многократного использования, в соответствии с требованиями эксплуатационно-технической документации на СКЗИ с составлением акта о списании и уничтожении ключевых материалов.

29. При обнаружении бракованных криптографических ключей один экземпляр бракованного изделия следует возвратить удостоверяющему центру для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от изготовителя.

30. Ключевые носители, журнал учёта СКЗИ и журнал учёта ключей должны храниться в сейфе в помещении для хранения СКЗИ.

31. Криптографические ключи при необходимости сдаются пользователем СКЗИ на временное хранение уполномоченному лицу.

IV. Использование СКЗИ и криптографических ключей

32. Криптографические ключи используются для обеспечения конфиденциальности, авторства и целостности электронных документов.

33. Для шифрования электронного документа пользователь СКЗИ должен

использовать свой криптографический ключ.

34. Проверка подлинности электронной подписи электронного документа осуществляется пользователем СКЗИ с использованием открытой части криптографического ключа отправителя документа.

35. Расшифрование электронного документа осуществляется с использованием закрытой части криптографического ключа пользователя СКЗИ и открытой части ключа отправителя документа.

36. Реализованные в СКЗИ алгоритмы шифрования в электронной подписи гарантируют невозможность восстановления закрытой части криптографических ключей отправляемых электронных документов с открытой частью криптографических ключей.

37. Во время работы с ключевыми носителями доступ к ним посторонних лиц должен быть исключён.

38. Ключевой носитель должен быть вставлен в считывающее устройство только на время выполнения операций формирования и проверки электронной подписи, шифрования и расшифрования. Размещение ключевого носителя в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

39. Криптографический ключ невозможно использовать, если истёк срок действия.

40. Криптографический ключ на ключевом носителе должен защищаться паролем.

41. Ответственность за сохранение пароля в тайне возлагается на пользователя СКЗИ.

42. При выявлении сбоев или отказов, компрометации криптографических ключей пользователь СКЗИ обязан сообщить о факте их возникновения администратору безопасности за эксплуатацию СКЗИ и предоставить ему ключевой носитель криптографических ключей для проверки их работоспособности. Проверку работоспособности ключевых носителей с ключевой информацией выполняет уполномоченное лицо.

43. В случае если рабочие криптографические ключи потеряли работоспособность пользователь СКЗИ делает копию ключевого носителя, используя резервные криптографические ключи, с последующим уведомлением администратора безопасности за эксплуатацию СКЗИ.

44. При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптографических ключей, указанные сообщения необходимо передавать только с использованием СКЗИ.

V. Изготовление и плановая смена криптографических ключей

45. Подготовку документов для изготовления и смены криптографических ключей в удостоверяющих центрах производят уполномоченные лица.

46. Криптографические ключи изготавливаются на отчуждаемый ключевой носитель (дискету, ruToken, Etoken и др.) в соответствии с эксплуатационно-технической документацией на СКЗИ и требованиями безопасности, установленными настоящей Инструкцией.

47. После получения новых ключевых носителей с ключевой информацией создаются резервные криптографические ключи в двух экземплярах для исключения утраты ключевой информации вследствие дефектов носителей.

48. В целях обеспечения непрерывности проведения работы плановую смену криптографических ключей следует производить заблаговременно (за 10 дней до окончания срока действия закрытой части криптографических ключей).

49. Переход на новые криптографические ключи пользователь СКЗИ в соответствии с эксплуатационно-технической документацией на СКЗИ выполняет совместно с уполномоченными лицами в сроки, указанные в сертификате криптографического ключа.

50. При замене криптографических ключей используется программное обеспечение в соответствии с эксплуатационно-технической документацией на СКЗИ. Пользователь СКЗИ самостоятельно обновляет сертификат ключа подписи на АРМ. Обновление справочников сертификатов ключей подписи осуществляется в соответствии с эксплуатационно-технической документацией на СКЗИ.

VI. Действия при компрометации криптографических ключей

51. К обстоятельствам, указывающим на возможную компрометацию криптографических ключей, но не ограничивающим их, относятся следующие:

1) потеря ключевых носителей с рабочими и/или резервными криптографическими ключами;

2) потеря ключевых носителей с рабочими и/или резервными криптографическими ключами с последующим их обнаружением;

3) передача ключевой информации по каналам связи в открытом виде;

4) возникновение подозрений относительно утечки информации или её искажения;

5) утрата ключей от сейфов и помещений в момент нахождения в них ключевых носителей с рабочими и/или резервными криптографическими ключами;

6) временный доступ посторонних лиц к ключевым носителям, а также другие события, при которых достоверно неизвестно, что произошло с ключевыми носителями.

52. В случае возникновения обстоятельств, указанных в пункте 51 настоящей Инструкции, пользователь СКЗИ обязан незамедлительно прекратить обмен электронными документами с использованием скомпрометированных криптографических ключей, по телефону информировать администратора безопасности за эксплуатацию СКЗИ о факте

компрометации используемых криптографических ключей.

53. В чрезвычайных случаях, когда отсутствуют криптографические ключи для замены скомпрометированных, допускается использование скомпрометированных криптографических ключей. В этом случае период использования скомпрометированных криптографических ключей должен быть максимально коротким, а передаваемая информация как можно менее ценной.

54. Решение о компрометации криптографических ключей принимает администратор безопасности за эксплуатацию СКЗИ. Пользователь СКЗИ предоставляет письменное объяснение о факте компрометации криптографических ключей.

55. Письменное объяснение должно содержать:

1) идентификационные параметры скомпрометированного криптографического ключа;

2) фамилию, имя, отчество пользователя СКЗИ, который владел скомпрометированным криптографическим ключом;

3) сведения об обстоятельствах компрометации криптографического ключа;

4) время и обстоятельства выявления факта компрометации криптографического ключа.

56. После принятия решения о компрометации криптографического ключа принимаются меры об изъятии из обращения и замене его на новый криптографический ключ. Уполномоченное лицо проводит работу по отзыву сертификата ключа подписи пользователя СКЗИ. Данный сертификат ключа подписи, соответствующий скомпрометированному криптографическому ключу пользователя СКЗИ, помещается в список отозванных сертификатов.

57. Дата, начиная с которой сертификат криптографического ключа считается недействительным, устанавливается равной дате формирования списка отозванных сертификатов, в который был включён отзываемый сертификат криптографического ключа.

58. Сертификат криптографического ключа, соответствующий скомпрометированному криптографическому ключу, должен храниться у уполномоченных лиц в течение срока хранения электронных документов для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением электронной подписи.

59. Использование СКЗИ может быть возобновлено только после ввода в действие другого криптографического ключа взамен скомпрометированного.

VII. Изъятие и уничтожение СКЗИ и криптографических ключей

60. Неиспользованные или выведенные из действия криптографические ключи подлежат выводу из эксплуатации и уничтожаются в установленные сроки. Вместе с выводимыми из эксплуатации СКЗИ подлежит уничтожению эксплуатационно-техническая документация на СКЗИ.

61. Уничтожение криптографических ключей на ключевых носителях и

СКЗИ производит уполномоченное лицо.

62. СКЗИ подлежат изъятию из аппаратных средств, на которых они функционировали в случае:

увольнение пользователя;

отстранение пользователя от исполнения обязанностей, связанных с использованием СКЗИ;

уничтожения СКЗИ в связи с окончанием срока действия или заменой программного обеспечения.

При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационно-технической документацией на СКЗИ процедура удаления программного обеспечения СКЗИ, и они полностью отсоединены от аппаратных средств.

63. Криптографические ключи, находящиеся на ключевых носителях, уничтожаются путём физического уничтожения ключевого носителя, на котором они записаны или путём стирания (разрушения, переформатирования) ключевых носителей средствами программного обеспечения СКЗИ по технологии, принятой для многократного использования в соответствии с требованиями эксплуатационно- технической документации на СКЗИ.

64. Бумажная и прочая сгораемая ключевая информация, а также эксплуатационно-техническая документация на СКЗИ уничтожается путём сжигания или перерабатывается с помощью бумагорезательных машин (измельчения).

65. СКЗИ, ключевая информация должны быть уничтожены в сроки, указанные в эксплуатационно-технической документации на СКЗИ. Если срок уничтожения эксплуатационно-технической документацией на СКЗИ не установлен, то бумажная ключевая информация должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). При уничтожении составляется Акт о списании и уничтожении средств криптографической защиты.

66. При уничтожении криптографических ключей, находящихся на ключевых носителях, необходимо:

1) установить наличие оригинала и всех копий ключевых носителей путём сверки с записями в журнале учёта ключей;

2) убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;

3) произвести уничтожение ключевой информации на оригинале и всех копиях ключевых носителей.

67. В журнале учёта ключей производится отметка об уничтожении криптографических ключей.

68. Уничтожение криптографических ключей и СКЗИ производится постоянно действующей технической комиссией по защите информации Министерства с оформлением акта о списании и уничтожении СКЗИ либо акта о списании и уничтожении ключевых материалов. Акт утверждается председателем постоянно действующей технической комиссии по защите

информации Министерства.

69. О проведённом изъятии делается отметка в журнале учёта СКЗИ.

70. О проведённом уничтожении делается отметка в журнале учёта СКЗИ либо журнале учёта ключей.

VIII. Организация безопасной эксплуатации СКЗИ и обеспечение безопасности информации

71. При использовании АРМ с установленными СКЗИ, подключёнными к информационно-телекоммуникационным сетям общего пользования, с целью исключения возможности несанкционированного доступа к среде функционирования СКЗИ, компонентам СКЗИ, а также к системным ресурсам используемых операционных систем со стороны указанных сетей, должны выполняться требования Указа Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» и требования, определённые в соответствии с принятой в Министерстве политикой информационной безопасности информационных систем персональных данных.

72. На АРМ, подлежащих оснащению СКЗИ, должно использоваться только лицензионное программное обеспечение фирм-производителей.

73. Перед установкой СКЗИ необходимо проверить программное обеспечение АРМ на отсутствие вирусов и программных закладок и удалить все неиспользуемые общие ресурсы на АРМ, в том числе и создаваемые по умолчанию.

74. На АРМ не должны устанавливаться средства разработки программного обеспечения и программы-отладчики. Если наличие средства отладки приложений обусловлено технологическими потребностями, то его использование должно быть согласовано с администратором безопасности за эксплуатацию СКЗИ. При этом должны быть реализованы меры, исключающие возможность использования этих средств для просмотра и редактирования кода и памяти приложений, использующих СКЗИ.

75. Для обеспечения защиты от несанкционированного доступа (далее – НСД) в соответствии с правилами пользования СКЗИ используются средства защиты от НСД, сертифицированные Федеральной службой безопасности Российской Федерации.

76. Настройку средств защиты от НСД на требуемую конфигурацию выполняет уполномоченное лицо. Настройка должна исключать возможность вмешательства пользователя СКЗИ в процессы загрузки операционной системы, прикладного программного обеспечения и проверки целостности программной среды.

77. При отсутствии возможности применения программно-аппаратных средств защиты от НСД (например, из-за конструктивных особенностей)

допускается защиту информации от НСД производить за счёт следующих дополнительных организационных мер:

1) размещение указанных СКЗИ в аттестованном, специально выделенном помещении (серверной);

2) запирание на замок и опечатывание двери в случае отсутствия необходимости санкционированного доступа в указанное помещение;

3) допуск в указанное помещение только сотрудников, назначенных приказом Министерства (указанные сотрудники не должны иметь доступ к настройкам СКЗИ);

4) блокировка разъёмов для подключения монитора и манипулятора «мышь»;

5) контроль целостности установленного программного обеспечения с помощью программ контроля целостности, входящих в комплект размещённого в помещении СКЗИ.

78. Из состава системы должно быть удалено всё оборудование, которое может создавать угрозу операционной системе.

79. На АРМ должна устанавливаться только одна операционная система. Не должны использоваться нестандартные, измененные или отладочные версии операционных систем.

80. В случае использования АРМ несколькими сотрудниками с различными криптографическими ключами необходимо производить выгрузку ключевой информации (перезагрузку АРМ).

81. На время длительного отсутствия пользователя СКЗИ его АРМ должно быть выключено. При необходимости, по согласованию с администратором безопасности за эксплуатацию СКЗИ АРМ на период отсутствия пользователя СКЗИ может быть использовано вновь назначенным пользователем СКЗИ со своим индивидуальным криптографическим ключом.

IX. Организация режима в помещениях, где установлены и хранятся СКЗИ и криптографические ключи

82. Размещение, охрана и организация режима в помещениях, где установлены и хранятся СКЗИ, криптографические ключи (далее – Помещения) должны обеспечивать сохранность персональных данных, СКЗИ, криптографических ключей и исключать возможность неконтролируемого проникновения или пребывания в Помещениях посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

83. При размещении и монтаже СКЗИ в Помещениях, а также другого оборудования, функционирующего с СКЗИ, необходимо свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам.

84. Помещения выделяются с учётом размеров контролируемых зон. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие дверей в нерабочее время.

85. Для предотвращения просмотра извне Помещений окна должны быть защищены шторами, жалюзи и т.д. или экраны мониторов должны быть повернуты в противоположную сторону от окна.

86. На время отсутствия пользователя СКЗИ криптографические ключи должны быть убраны в сейф или, по согласованию с администратором безопасности за эксплуатацию СКЗИ, необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами.

87. Режим охраны Помещений, в том числе правила допуска сотрудников Министерства и посетителей в рабочее и нерабочее время, устанавливается правовыми документами Министерства.

88. Входные двери в Помещения должны быть оборудованы замками, обеспечивающими их открытие только для санкционированного прохода, а также средствами для опечатывания.

89. Для обеспечения безопасного хранения СКЗИ, дистрибутивов СКЗИ, эксплуатационно-технической документации на СКЗИ, криптографических ключей, ключей от Помещений пользователь СКЗИ обеспечивается:

1) пеналом (тубусом) с приспособлением для опечатывания;

2) пломбиром, который должен находиться непосредственно у пользователя СКЗИ, осуществляющего опечатывание;

3) сейфом с приспособлением для опечатывания или дополнительным кодовым замком.

90. Учёт опечатывающих устройств ведётся в Журнале учёта опечатывающих устройств.

91. Пеналы (тубусы) нумеруются в соответствии со структурой учётного номера K/N, где: K – номер помещения, N – порядковый номер пенала (тубуса), который наносится с помощью этикетки (маркера).

92. Ключи от замков входных дверей Помещений нумеруются в соответствии со структурой учётного номера – K/N, где: K – номер помещения, N – номер экземпляра ключа.

93. Ключи от замков входных дверей Помещений (оригиналы и дубликаты) учитываются и выдаются в Журнале учёта ключей (дубликатов ключей) от помещений, где хранятся и установлены средства криптографической защиты информации и металлических шкафов (сейфов) по форме согласно приложению 13.

94. Один экземпляр ключа от помещения, где установлены СКЗИ должен находиться у пользователя СКЗИ, работающего в этом помещении.

95. Дубликаты ключей от помещений, где установлены СКЗИ сдаются уполномоченному лицу с отметкой в Журнале учёта ключей (дубликатов ключей) от помещений, где хранятся и установлены средства криптографической защиты информации и металлических шкафов (сейфов).

96. Помещения, где установлены СКЗИ и опечатанные сейфы, могут быть вскрыты только пользователем СКЗИ или в их отсутствие администратором безопасности за эксплуатацию СКЗИ.

97. Один экземпляр ключа от входной двери помещения для хранения СКЗИ должен находиться у сотрудника, на которого возложены обязанности по организации криптографической защиты.

98. Дубликаты ключей от входной двери помещения для хранения СКЗИ хранятся в сейфе министра социальной политики и труда Удмуртской Республики (далее – министр).

99. Помещение для хранения СКЗИ и находящиеся в нём опечатанные сейфы могут быть вскрыты только уполномоченным лицом.

100. В случае утраты рабочих экземпляров ключей от Помещений дубликаты ключей выдаются для вскрытия Помещений. Осуществляется замена замка (секрета замка). Ключи от нового замка подлежат учёту в Журнале учёта ключей (дубликатов ключей) от помещений, где хранятся и установлены СКЗИ и металлических шкафов (сейфов).

101. При обнаружении признаков, указывающих на возможное несанкционированное проникновение посторонних лиц в Помещения, о случившемся должно быть немедленно сообщено администратору безопасности за эксплуатацию СКЗИ. Администратор безопасности за эксплуатацию СКЗИ должен оценить возможность компрометации хранящихся криптографических ключей и принять, при необходимости, меры к локализации последствий компрометации криптографических ключей и к их замене. Уполномоченное лицо составляет Акт несанкционированного проникновения в помещение или металлический шкаф (сейф) по форме согласно приложению 14.

102. Хранение ключей от Помещений вне Министерства не допускается.

103. В начале рабочего дня пользователь СКЗИ, уполномоченное лицо:

1) получают опечатанные тубусы под расписку в Журнале приёма (сдачи) под охрану помещений, где установлены и хранятся средства криптографической защиты информации, ключевые материалы, металлические шкафы (сейфы) по форме согласно приложению 15 в службе охраны Министерства;

2) проверяют целостность опечатывания Помещения и открывают замок с использованием ключа.

104. По окончании рабочего дня пользователь СКЗИ, уполномоченное лицо:

1) опечатывают Помещения пломбиром или ярлыком по форме согласно приложению 16;

2) сдают рабочие экземпляры ключей от Помещений в опечатанных тубусах под расписку в Журнале приёма (сдачи) под охрану помещении, где установлены и хранятся СКЗИ, ключевые материалы, металлические шкафы (сейфы), в службу охраны Министерства.

X. Порядок доступа к сейфам

105. Для хранения ключевых материалов, эксплуатационно-технической

документации на СКЗИ, дистрибутивов используемых СКЗИ в Помещении для хранения СКЗИ должно быть установлено необходимое число надёжных сейфов.

106. Сейфы должны быть оборудованы внутренними замками с двумя экземплярами ключей и (или) кодовыми замками либо приспособлениями для опечатывания замочных скважин (допустимо использование ярлыка по форме согласно приложению 17).

107. Пользователь СКЗИ хранит ключевые материалы в сейфе.

108. Для доступа к содержимому сейфа с отрудник, ответственный за данный сейф, проверяет целостность сейфа, открывает механический замок с использованием ключа.

109. Пломбир, предназначенный для опечатывания сейфа, должен находиться у сотрудника, ответственного за данный сейф.

110. Рабочие ключи от сейфов нумеруются в соответствии со структурой учётного номера K/N, где: K – номер сейфа, N – номер экземпляра ключа и предоставляются сотруднику, ответственному за данный сейф, под роспись в Журнале учёта ключей (дубликатов ключей) от помещений, где хранятся и установлены СКЗИ и металлических шкафов (сейфов).

111. Дубликаты ключей от сейфов пользователей СКЗИ хранятся в сейфе уполномоченного лица.

112. Дубликаты ключей от сейфа администратора безопасности за эксплуатацию СКЗИ хранятся в сейфе министра в опечатанном пенале (тубусе).

113. Ключи от сейфа не должны передаваться сотрудникам, не ответственным за данный сейф.

114. Опечатанный сейф пользователя СКЗИ может быть вскрыт только самим пользователем СКЗИ. В исключительных случаях разрешается вскрытие сейфа специально назначенной комиссией по указанию министра.

115. При утрате ключа от сейфа замок данного сейфа необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от сейфа переделать невозможно, то такой сейф необходимо заменить. Об утрате ключа пользователь СКЗИ должен немедленно сообщить администратору безопасности за эксплуатацию СКЗИ. Порядок хранения документов в сейфе, от которого утрачен ключ, до изменения секрета замка устанавливает администратор безопасности за эксплуатацию СКЗИ.

116. При увольнении сотрудника либо при назначении другого лица ответственным за сейф сотрудник обязан сдать имеющиеся у него ключи от сейфа уполномоченному лицу.

117. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в сейф посторонних лиц, о случившемся должно быть немедленно сообщено администратору безопасности за эксплуатацию СКЗИ. Администратор безопасности за эксплуатацию СКЗИ должен оценить возможность компрометации, хищения, подмены, порчи хранящихся документов и технических средств и принять, меры к локализации

последствий с составлением акт несанкционированного проникновения в помещение или металлическом шкафе (сейфов).

118. По окончании рабочего дня пользователь СКЗИ, уполномоченное лицо:

1) опечатывают сейф пломбиром или ярлыком;

2) сдают рабочие экземпляры ключей от сейфов в опечатанном пенале (тубусе) под роспись в Журнале приёма (сдачи) под охрану помещений, где установлены и хранятся СКЗИ, ключевые материалы, металлические шкафы (сейфы), в службу охраны Министерства.

XI. Контроль безопасности СКЗИ

119. Текущий контроль за организацией и обеспечением функционирования СКЗИ, предусмотренных эксплуатационно-технической документацией на СКЗИ, возлагается на администратора безопасности за эксплуатацию СКЗИ в пределах его полномочий.

XII. Ответственность за неисполнение требований по эксплуатации СКЗИ и криптографических ключей

120. Пользователь СКЗИ и уполномоченное лицо несут персональную ответственность за неисполнение требований настоящей Инструкции в соответствии с действующим законодательством Российской Федерации.

Приложение 1
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

УТВЕРЖДАЮ
Председатель Технической
комиссии по защите информации
_____ И.О. Фамилия
«____» _____ _____ г.

АКТ № _____
ввода в эксплуатацию средств криптографической защиты информации (ПО VipNet Client)

«____» _____ _____ г. город Ижевск

Техническая комиссия по защите информации, созданная на основании приказа Минсоцполитики УР от «____» _____ _____ года № _____, в присутствии ответственного за эксплуатацию защищённой сети передачи данных VipNet № 577 Минсоцполитики УР (администратор безопасности защищённой сети VipNet № 577) _____,
(Фамилия, имя, отчество)

составила акт о том, что программное обеспечение VipNet Client установлено в Минсоцполитики УР, расположенном по адресу: 426004, г. Ижевск, ул. Ломоносова, 5, в помещении № _____, охрана и организация режима в помещении, в котором установлено программное обеспечение VipNet Client, а также условия хранения установочных дистрибутивов программного обеспечения VipNet Client, эксплуатационно-технической документации к программному обеспечению VipNet Client, ключевых документов, соответствуют установленным требованиям.

Программное обеспечение VipNet Client установлено и настроено в соответствии с эксплуатационно-технической документацией и введено в эксплуатацию. Поэкземплярный учёт используемых средств криптографической защиты информации, эксплуатационно-технической документации к ним, ключевых документов организован.

Формуляр ФРКЕ.00004-05 30 01 ФО выведен на бумажный носитель, раздел 10 Формуляра заполнен установленным порядком. Формуляр передан на хранение в соответствии с разделом 9 Формуляра.

Пользователь СКЗИ _____
(Фамилия, имя, отчество пользователя СКЗИ)

обучен правилам работы с программным обеспечением VipNet Client и ознакомлен с регламентирующими документами. Пользователь СКЗИ допущен к самостоятельным действиям с использованием программного обеспечения VipNet Client на основании проведённого тестирования и проверки его результатов (Приложение к акту от «__» _____ ____ года № _____).

_____ _____ /_____
(должность пользователя СКЗИ) (подпись) (Фамилия И.О.)

_____
(дата)

Абонентский пункт с установленным программным обеспечением VipNet Client имеет следующие характеристики:

1. Системный блок №: _____.
2. Программное обеспечение VipNet C lient вер сия _____ сборка _____.
3. Системное программное обеспечение - операционная система:

- наименование и версия _____.
- код _____.

4. Дополнительно установленное программное обеспечение:

- антивирусное: _____.
- для удалённого администрирования: _____.
- прикладное: _____.

Абонентский пункт защищённой сети передачи данных VipNet № 577 Минсоцполитики УР отвечает требованиям по обеспечению безопасности обмена конфиденциальной информацией.

Настоящий акт составлен в 1 экземпляре.

Члены комиссии:

_____ / _____
(должность) (подпись) (Фамилия И.О.)

_____ / _____
(должность) (подпись) (Фамилия И.О.)

_____ / _____
(должность) (подпись) (Фамилия И.О.)

_____ / _____
(должность) (подпись) (Фамилия И.О.)

Приложение 2
к Инструкции по обеспечению
безопасности эксплуатации
шифровальных (криптографических)
средств в информационных системах
Министерства социальной политики и
труда Удмуртской Республики

Форма

УТВЕРЖДАЮ
Председатель Технической
комиссии по защите информации
_____ И.О. Фамилия
«____» _____ _____ г.

АКТ № _____
ввода в эксплуатацию средств криптографической защиты информации

«____» _____ _____ г. город Ижевск

Техническая комиссия по защите информации, созданная на основании приказа Минсоцполитики УР от «____» _____ _____ года № _____, составила настоящий акт на основании приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации 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 содержащее сведений, составляющих государственную тайну».

Средство криптографической защиты информации (далее – СКЗИ) установлено для работы с органами государственной власти, территориальными органами Минсоцполитики УР, подведомственными Минсоцполитики УР организациями и иными сторонними организациями, входящими в систему защищённого электронного документооборота для реализации защищённого информационного взаимодействия в соответствии с договорами и соглашениями, предусмотренными регламентами.

Размещение автоматизированного рабочего места с организованным защищённым документооборотом (далее – АРМ-ЗЭД) в Минсоцполитики УР, установленного на средстве вычислительной техники инвентаризационный номер _____, расположенном в помещении № _____ административного здания по адресу: г. Ижевск, ул. Ломоносова, дом 5, специальное оборудование, охрана и организация режима в помещении, в котором размещён АРМ-ЗЭД, а также условия хранения инсталлирующих

СКЗИ носителей, эксплуатационно-технической документации на СКЗИ, ключевых документов, соответствуют установленным требованиям.

№ п/п	Наименование	Серийный номер	Заводской или инвентарный номер системного блока

Установка и настройка СКЗИ проведена в соответствии с требованиями, поэкземплярный учёт используемых СКЗИ, эксплуатационно-технической документации к ним, ключевых документов организован.

АРМ-ЗЭД отвечает требованиям по обеспечению безопасности обмена конфиденциальной информацией.

Формуляр _____ выведен на бумажный носитель, раздел 11 Формуляра заполнен установленным порядком. Формуляр передан на хранение в соответствии с разделом 10 Формуляра.

Пользователь СКЗИ _____
(Фамилия, имя, отчество)

обучен правилам работы с СКЗИ и ознакомлен с эксплуатационно-технической документацией на СКЗИ и регламентирующими документами. Пользовател ь СКЗИ допущен к самостоятельным действиям с использованием СКЗИ на основании проведённого тестирования и проверки его результатов (Приложение к акту от «__» _____ ____ года № _____).

_____ _____ /_____
(должность пользователя СКЗИ) (подпись) (Фамилия И.О.)

_____
(дата)

Настоящий акт составлен в 1 экземпляре.

Члены комиссии:

_____ _____ /_____
(должность) (подпись) (Фамилия И.О.)

_____ _____ /_____
(должность) (подпись) (Фамилия И.О.)

_____ _____ /_____
(должность) (подпись) (Фамилия И.О.)

_____ _____ /_____
(должность) (подпись) (Фамилия И.О.)

_____

Приложение 3
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

ЖУРНАЛ
учёта пользователей средств криптографической защиты информации

№ п\п	Сведения о допуске к СКЗИ				Сведения о прекращении допуска к СКЗИ		
	Наименование СКЗИ	Документ, на основании которого предоставлен допуск	Фамилия И.О. лица, допущенного к работе с СКЗИ	Должность лица, допущенного к работе с СКЗИ	Документ, на основании которого прекращён допуск	Фамилия И.О. и должность лица, прекращающего работу с СКЗИ	Дата и подпись лица об ознакомлении с документом, на основании которого прекращён допуск к работе с СКЗИ
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**

Приложение 4
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

ЖУРНАЛ
инструктажа пользователей информационных систем персональных данных (ИСПДн)

№ п\п	Дата проведения инструктажа	Фамилия И.О. пользователя ИСПДн	Дата приёма на работу	Номер ИСПДн	С приказами ознакомлен(а) (реквизиты приказа)	Подпись пользователя ИСПДн	Сотрудник, ответственный за проведение инструктажа пользователей ИСПДн	
							Фамилия И.О.	подпись
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**

Приложение 5
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

УТВЕРЖДАЮ
Председатель Технической
комиссии по защите информации
_____ И.О. Фамилия
«____» _____ 201_ г.

АКТ ____
об изъятии средств криптографической защиты информации из аппаратных средств

Техническая комиссия по защите информации, созданная на основании приказа Минсоцполитики УР от «___» _____ 201_ года № ____, на основании приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации 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 содержащее сведений, составляющих государственную тайну» составила настоящий акт о том, что «___» _____ 201__ года следующие средства криптографической защиты информации (далее – СКЗИ) изъяты из аппаратных средств:

№ п/п	Наименование СКЗИ	Место установки СКЗИ	Номера аппаратных средств, в которые установлены или к которым были подключены СКЗИ	Фамилия И.О. пользователя
1	2	3	4	5

Всего выведено их эксплуатации _____ комплектов СКЗИ.
(прописью)

Настоящий акт составлен в 1 экземпляре.

Члены комиссии:

_____ (должность)	_____ (подпись)	/ _____ (Фамилия И.О.)
_____ (должность)	_____ (подпись)	/ _____ (Фамилия И.О.)
_____ (должность)	_____ (подпись)	/ _____ (Фамилия И.О.)
_____ (должность)	_____ (подпись)	/ _____ (Фамилия И.О.)

Отметки в журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним об изъятии СКЗИ произвел:

_____ _____
Ф. И. О. подпись

«___» _____ 2018 г.

Приложение 6
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

УТВЕРЖДАЮ
Председатель Технической
комиссии по защите информации
_____ И.О. Фамилия
«____» _____ _____ г.

АКТ № _____
о списании и уничтожении средств
криптографической защиты информации

«____» _____ _____ г. город Ижевск

Техническая комиссия по защите информации, созданная на основании приказа Минсоцполитики УР от «____» _____ _____ года № _____, составила настоящий акт на основании приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с исполнением средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

В связи с окончанием срока действия сертификата соответствия требованиям Федеральной службы безопасности Российской Федерации уничтожены следующие средства криптографической защиты информации (далее – СКЗИ):

№ п/п	Наименование СКЗИ, эксплуатационно-технической документации к ним	Серийные номера СКЗИ, эксплуатационно-технической документации к ним	Номера экземпляров (криптографические номера) ключевых документов	Срок действия сертификата соответствия требованиям ФСБ России	Пользователь СКЗИ	
					Фамилия И. О.	Подпись

Всего уничтожено _____ наименований СКЗИ в количестве _____ экземпляров.

Отметка об уничтожении СКЗИ в Журнале поэкземплярного учёта СКЗИ, эксплуатационно-технической документации к ним произведена.

Настоящий акт составлен в 1 экземпляре.

Члены комиссии:

_____ / _____
(должность) (подпись) (Фамилия И.О.)

_____ / _____
(должность) (подпись) (Фамилия И.О.)

_____ / _____
(должность) (подпись) (Фамилия И.О.)

_____ / _____
(должность) (подпись) (Фамилия И.О.)

Приложение 7
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

УТВЕРЖДАЮ
Председатель Технической
комиссии по защите информации
_____ И.О. Фамилия
«____» _____ _____ г.

АКТ № _____
о списании и уничтожении ключевых материалов

«____» _____ _____ г. город Ижевск

Техническая комиссия по защите информации, созданная на основании приказа Минсоцполитики УР от «____» _____ _____ года № _____, составила настоящий акт на основании приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с исполнением средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Список сертификатов открытых ключей и электронных ключевых носителей, соответствующих установленным требованиям, подготовленных к списанию и уничтожению.

Уничтожены ключевые материалы (ключи) в количестве _____ экземпляров.

№ п/п	Номера серий ключевых материалов		Номера экземпляров ключевых материалов	Владелец ключевых материалов		Срок действия ключевых материалов (срок «с» и «по»)	Фамилия, И. О. лица (наименование организации), изготовившего ключевые материалы
	Регистрационный номер ключевых носителей	Серийный номер сертификатов ключей		Фамилия, И. О.	Подпись		

Копии ключевых материалов (носителей) в количестве _____ экземпляров уничтожены.

Уничтожение ключевых материалов (носителей) производилось путём физического уничтожения.

Отметка об уничтожении ключевых материалов (носителей) в Журнале поэкземплярного учёта ключевых материалов произведена.

Настоящий акт составлен в 1 экземпляре.

Члены комиссии:

(должность)	(подпись)	/ (Фамилия И.О.)
(должность)	(подпись)	/ (Фамилия И.О.)
(должность)	(подпись)	/ (Фамилия И.О.)
(должность)	(подпись)	/ (Фамилия И.О.)

Приложение 8
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

ЖУРНАЛ
учёта опечатывающих устройств

№ п/п	Наименование опечатывающего устройства и его содержимое	Номер опечатывающего устройства	Отметка о получении опечатывающих устройств		Отметка о возврате опечатывающих устройств		Примечание
			Фамилия И.О. пользователя	Дата, подпись	Фамилия И.О. пользователя	Дата, подпись	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**

Приложение 9
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

ЖУРНАЛ
проверки установленных средств криптографической защиты информации на автоматизированном рабочем месте

№ п/п	Наименование СКЗИ	Информация об установленном СКЗИ			Дата и время проверки	Сотрудник, проводивший проверку		Результат проверки	Примечание
		№ помещения	Инвентарный номер АРМ	Ключевые материалы		Фамилия И.О.	Подпись		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

Приложение 10

к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

форма

ЖУРНАЛ

поэкземплярного учёта средств криптографической защиты информации, эксплуатационно-технической документации к ним

№ п/п	Наименование СКЗИ, эксплуатационно-технической документации к ним	Серийные номера СКЗИ, эксплуатационно-технической документации к ним	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств и уничтожении			Примечание
				От кого получены	Дата и номер сопроводительного письма	Фамилия И.О. пользователя СКЗИ	Дата и расписка в получении	Фамилия 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)	Фамилия И.О. сотрудника органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписки об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение 11

к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

ЖУРНАЛ
поэкземплярного учёта ключевых материалов

№ п/п	Наименование ключевых материалов	Номера серий ключевых материалов		Номера экземпляров (криптографические номера) ключевых материалов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) ключевых материалов			Отметка об изъятии ключевых материалов из аппаратных средств и уничтожении			Примечание
		Регистрационный номер ключевых носителей	Серийный номер сертификатов ключей		От кого получены	Дата и номер сопроводительного письма	Фамилия И.О. пользователя ключевых материалов	Дата и расписка в получении	Фамилия, Имя, Отчество сотрудника органа криптографической защиты информации, пользователя ключевыми материалами, производивших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены ключевые материалы	Дата изъятия (уничтожения)	Фамилия, Имя, Отчество сотрудника органа криптографической защиты, пользователя ключевыми материалами, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Приложение 12
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

ЖУРНАЛ
учёта и выдачи средств криптографической защиты информации, ключевых материалов, ключей от сейфов и металлических шкафов

№ п/п	Наименование СКЗИ, ключевых материалов, ключей от сейфов и металлических шкафов	Номер СКЗИ, ключевых материалов, ключей от сейфов и металлических шкафов	Отметка о получении СКЗИ информации, ключевых материалов, ключей от сейфов и металлических шкафов		Отметка о возврате СКЗИ, ключевых материалов, ключей от сейфов и металлических шкафов		Примечание
			Дата и время	Подпись	Дата и время	Подпись	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**

Приложение 13
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

ЖУРНАЛ
учёта ключей (дубликатов ключей) от помещений, где хранятся и установлены средства криптографической защиты информации и металлических шкафов (сейфов)

№ п/п	Номер помещения (сейфа)*	Ключ		Отметка о выдаче			Сотрудник, на которого возложены обязанности по организации криптографической защиты информации		Отметка об изъятии		Примечание
		Номер ключа	Оригинал/ дубликат	Фамилия И.О. сотрудника	Дата	Подпись	Фамилия И.О.	Подпись	Дата изъятия	Фамилия И.О. сотрудника	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**

Примечание:
* перед номером помещения (сейфа) указать префикс: С – сейф, П – помещение.

Приложение 14
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

УТВЕРЖДАЮ
Председатель Технической
комиссии по защите информации
_____ И.О. Фамилия
«____» _____ _____ г.

АКТ № _____
несанкционированного проникновения в помещение или металлический шкаф (сейф)

«____» _____ _____ г. город Ижевск

Техническая комиссия по защите информации, созданная на основании приказа Минсоцполитики УР от «____» _____ _____ года № _____, составила настоящий акт о том, что «__» _____ _____ г. произошло несанкционированное проникновение в опечатанное (ый) _____ _____ № _____ в Минсоцполитики УР, расположенном по адресу: 426004, г. Ижевск, ул. Ломоносова, 5.

О вскрытии были уведомлены:

_____ - _____;
_____ - _____;
_____ - _____.

В момент вскрытия _____ № _____ осмотр выявил:

_____
_____.

После вскрытия были допущены:

_____ - _____;
_____ - _____.

Приняты следующие меры:

_____

_____

_____

_____.

Настоящий акт составлен в 1 экземпляре.

Члены комиссии:

_____ / _____

(должность) (подпись) (Фамилия И.О.)

_____ / _____

(должность) (подпись) (Фамилия И.О.)

_____ / _____

(должность) (подпись) (Фамилия И.О.)

_____ /

(должность) (подпись) (Фамилия И.О.)

Приложение 15
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

ЖУРНАЛ
приёма (сдачи) под охрану помещений, где установлены и хранятся средства криптографической защиты информации, ключевые материалы, металлические шкафы (сейфы)

№ п/п	Дата сдачи/ получения	Время сдачи/получения	Номер тубуса	Номер пломбира	Подпись лица, сдавшего тубус	Подпись лица, принявшего тубус	Примечание
1	2	3	4	5	6	7	8

Приложение 16
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

Министерство социальной политики и труда Удмуртской Республики

_____

(наименование управления (отдела)

ОПЕЧАТАНО Кабинет № _____	Сотрудник _____ /_____/ Дата: ____._____.20____ г. Время: ____-____

_____

Приложение 17
к Инструкции по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики

Форма

Министерство социальной политики и труда Удмуртской Республики

_____

(наименование управления (отдела)

ОПЕЧАТАНО Шкаф № _____	Сотрудник _____/_____/ Дата: ____._____.20____ г. Время: ____-____

_____