АДМИНИСТРАЦИЯ ТАМБОВСКОЙ ОБЛАСТИ
ТАМБОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«МНОГОФУНКЦИОНАЛЬНЫЙ ЦЕНТР ПРЕДОСТАВЛЕНИЯ ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ УСЛУГ»
(ТОГКУ «МФЦ»)

ПРИКАЗ

« 20 »____12_____2017г. № 81.1-од

г. Тамбов

Об утверждении документов по обеспечению безопасности конфиденциальной информации с использованием средств криптографической защиты ТОГКУ «МФЦ»

Во исполнение требований Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативно-методического документа «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденного приказом Гостехкомиссии России от 30.08.2002 № 282,приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», руководящих документов ФСТЭК РФ по защите информации, содержащей персональные данные, и в целях обеспечения защиты информации и режима безопасности персональных данных работников учреждения и лиц, обращающихся за получением государственных и муниципальных услуг в Тамбовском областном государственном казенном учреждении «Многофункциональный центр предоставления государственных и муниципальных услуг» (далее – ТОГКУ «МФЦ»),

ПРИКАЗЫВАЮ:

1. Утвердить Положение об организации и проведении работ по обеспечению безопасности конфиденциальной информации с использованием средств криптографической защиты в ТОГКУ «МФЦ», далее – Положение (Приложение № 1).

2. Назначить ответственным за обеспечение безопасности хранения, обработки и передачи информации по каналам связи с использованием СКЗИ (ответственного пользователя средств криптографической защиты информации) в информационной системе ТОГКУ «МФЦ» – начальника информационно-технологического отдела ТОГКУ «МФЦ» Н.В. Буздина;

3. Утвердить инструкцию ответственного пользователя средств криптографической защиты информации в информационной системе ТОГКУ «МФЦ» (Приложение № 2).

4. Утвердить инструкцию по применению криптографических средств для защиты конфиденциальной информации в информационных системах ТОГКУ «МФЦ» (Приложение № 3).

5. Утвердить порядок доступа в помещения ТОГКУ «МФЦ», в которых ведется обработка персональных данных (Приложение № 4).

6. Утвердить Список лиц, допущенных к вскрытию и закрытию служебных помещений ТОГКУ «МФЦ», где установлены средства криптографической защиты информации или хранятся ключевые документы к ним (Приложение № 5).

7. Утвердить Инструкцию о порядке действий при компрометации криптоключей (Приложение № 6).

8. Утвердить состав комиссии по допуску пользователей к самостоятельной работе с СКЗИ (Приложение № 7).

9. Контроль за исполнением настоящего приказа возложить на заместителя директора Небогина А.М.

Директор ТОГКУ «МФЦ» Л.П. Третьякова

Согласовано:

Заместитель директора А.М. Небогин
«____»_____2017

Юрисконсульт отдела МТО С.А. Рябов
«____»_____2017

ПРИЛОЖЕНИЕ № 1
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от 20.12.2017 г. № 81.1-од

Положение
об организации и проведении работ пообеспечению безопасности конфиденциальной информации с использованием средств криптографической защиты в ТОГКУ «МФЦ»

1. Общие положения

1.1. Настоящий порядок разработан для практического применения пользователями средств криптографической защиты информации в ТОГКУ «МФЦ» и его филиалах «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ РФ от 13.06.2001 № 152, «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622, Приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.2. В ТОГКУ «МФЦ» определяются должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СКЗИ.

1.3. В ТОГКУ «МФЦ» разрабатываются нормативные и распорядительные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ.

2. Термины и определения

Средства криптографической защиты конфиденциальной информации, сертифицированные ФСБ, именуются – СКЗИ. К СКЗИ относятся криптографические алгоритмы преобразования информации, программные средства, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи включая СКЗИ, защиту от несанкционированного

доступа к информации и навязывания ложной информации, включая средства имитозащиты и «электронной подписи».

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

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

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

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

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

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

3. Порядок обращения с конфиденциальной информацией

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

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

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

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

3.4. Носители ключевой информации, ключевые документы и инсталлирующие СКЗИ носители должны храниться в шкафах (ящиках, хранилищах) индивидуального пользования, учтённых в соответствующем журнале (Приложение 1) в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.5. Не допускается: разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер; вставлять ключевой носитель в ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.), а также в дисководы других ПЭВМ;

записывать на ключевом носителе постороннюю информацию; вносить какие-либо изменения в программное обеспечение СКЗИ и ключевую информацию; модифицировать содержимое ключевых носителей; использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования; снимать несанкционированные копии с ключевых носителей; знакомить кого-либо с содержанием ключевых носителей или передавать кому-либо ключевые носители.

4. Требования по размещению СКЗИ и режиму охраны

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

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

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

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

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

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

4.7. Системные блоки ПЭВМ с СКЗИ оборудуются средствами контроля вскрытия (опломбируются).

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

5. Требования по обеспечению безопасности СКЗИ и ключевой информации

5.1. Ключевые и инсталляционные носители с программным обеспечением СКЗИ берутся на поэкземплярный учет в выделенных для этих целей журналах (Приложение 2).

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

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

5.4. Хранение ключевых и инсталляционных носителей с ПО СКЗИ

допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

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

6. Порядок допуска к самостоятельной работе с СКЗИ

6.1. К самостоятельной работе с СКЗИ допускаются лица, принятые на работу в ТОГКУ «МФЦ» в соответствии с приказом директора ТОГКУ «МФЦ» на основании заключенных с ними трудовых договоров и назначенные на должности, выполнение обязанностей по которым связано с изготовлением, хранением и использованием СКЗИ.

6.2. Сотрудники допускаются к самостоятельной работе с СКЗИ после их специальной подготовки (обучения) по утвержденным программам и сдачи зачета на допуск к самостоятельной работе с СКЗИ. Документом, подтверждающим должную специальную подготовку допускаемого и возможность его допуска к самостоятельной работе с СКЗИ является заключение (Приложение 3), составленное комиссией ТОГКУ «МФЦ» на основании принятого зачета по программе подготовки (обучения).

6.3. Программа подготовки к самостоятельной работе с СКЗИ (Приложение 4) содержит:

ознакомление с нормами действующего законодательства Российской Федерации, регулирующими отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; защите информации, прав субъектов, участвующих в информационных процессах и информатизации; использовании электронной подписи в электронных документах; ответственности за нарушение указанных норм;

ознакомление с нормативными актами органов государственного управления Российской Федерации, определяющими порядок разработки, производства, реализации, использования СКЗИ; регламентирующими вопросы взаимодействия участников информационного обмена с использованием СКЗИ; изучение должностных инструкций, положений о структурных подразделениях, других локальных нормативных актов ТОГКУ «МФЦ» по вопросам производственной деятельности, связанной с хранением и использованием СКЗИ; изучение эксплуатационно-технической документации на СКЗИ; приобретение практических навыков выполнения работ, предусмотренных обязанностями по занимаемой должности.

6.4. Методика подготовки к сдаче зачета на допуск к самостоятельной работе с СКЗИ должна предусматривать как формы самостоятельного изучения и

освоения программного материала работником, так и формы группового и индивидуального обучения с привлечением наиболее подготовленных специалистов ТОГКУ «МФЦ» в качестве преподавателей.

6.5. Пользователи, допущенные к работе с СКЗИ регистрируются в журнале учета обучения Пользователей СКЗИ (Приложение 5).

Приложение № 1
к Положению об организации и проведении работ
по обеспечению безопасности конфиденциальной информации
с использованием средств криптографической защиты в ТОГКУ «МФЦ»

Журнал
учета сейфов, металлических шкафов, спецхранилищ и ключей от них

Регистрационный номер	Наименование хранилища (сейф, металлический шкаф, кладовая, спецхранилище)	Заводской, инвентарный номер хранилища	Местонахождение хранилища (подразделение, номер комнаты, корпуса, здания)	Что хранится (документы, изделия)	Фамилия ответственного за хранилище	Количество Комплектов ключей и их номера	Расписка ответственного за хранилище в получении ключа и дата	Расписка в обратном приеме ключа и дата	Примечание
1	2	3	4	5	6	7	8	9	10

Приложение № 2
к Положению об организации и проведении работ
по обеспечению безопасности конфиденциальной информации
с использованием средств криптографической защиты в ТОГКУ «МФЦ»

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

№ 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		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении	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	примечание
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Примечание:
1. Журнал ведется специалистом, ответственным за эксплуатацию СКЗИ.
2. Тип съемных машинных носителей информации (МНИ), применяемых для хранения ключевой информации, определяется оператором.
3. В случае применения для хранения ключевой информации дискет ключевая информация записывается на две учтенные в журнале дискеты;
4. Надпись на дискетах с ключевой информацией предусматривает указание следующих сведений, примерно: «Ключ ЭП Новиковой Л.Н., учетный № 1, экз. № 1» или «Ключ аутентификации, учетный № 2, экз. № 1».
5. Уничтожение носителей ключей электронных подписей производится владельцами соответствующих ключей, уничтожение носителей ключа аутентификации производится специалистом ответственным за эксплуатацию СКЗИ.

Приложение № 3
к Положению об организации и проведении работ
по обеспечению безопасности конфиденциальной информации
с использованием средств криптографической защиты в ТОГКУ «МФЦ»

ЗАКЛЮЧЕНИЕ
о допуске к самостоятельной работе с СКЗИ

Место работы:_____
_____
Должность: _____
Фамилия, имя, отчество: _____
_____

с «____» _____ 20__ г. по «____»_____ 20 ___ г.

в соответствии с Программой, утвержденной приказом директора ТОГКУ «МФЦ» №_____ от "_____" _____ 201__ г., прошел(ла) подготовку по правилам работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну, количество часов – 10, и прошел(ла) тестирование _____, результат по итогам тестирования – _____.

По решению комиссии по допуску пользователей к самостоятельной работе с СКЗИ _____ допущен(а) / не допущен(а) к самостоятельной работе со средствами криптографической защиты информации.

Председатель комиссии: _____

Члены комиссии: _____

_____

_____

«____»_____20__ г.

Приложение № 4
к Положению об организации и проведении работ
по обеспечению безопасности конфиденциальной информации
с использованием средств криптографической защиты в ТОГКУ «МФЦ»

ПРОГРАММА

обучения работников ТОГКУ «МФЦ»
по правилам работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну

1. Общие положения

1.1. Настоящая программа разработана в соответствии с требованиями Инструкции «Об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну.

1.2. Программа предназначена для обучения пользователей СКЗИ ТОГКУ «МФЦ», а также пользователей СКЗИ – сотрудников организаций в рамках заключенных договоров по защищенному обмену электронными документами.

2. Темы занятий

2.1. Организация защиты информации при использовании СКЗИ

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

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи";
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением председателя Гостехкомиссии России от 30.03.1992г.);

- нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденный приказом Гостехкомиссии России от 30.08.2002 № 282;

- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ РФ от 13.06.2001 № 152.

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

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

- установление особого режима конфиденциальности;

- ограничение доступа к конфиденциальной информации;

- использование организационных мер и технических средств защиты информации;

- осуществление контроля за соблюдением установленного режима конфиденциальности.

Конкретное содержание указанных мероприятий для каждого отдельно взятого предприятия может быть различным по масштабам и формам. Это зависит в первую очередь от производственных, финансовых и иных возможностей предприятия, от объемов конфиденциальной информации и степени ее значимости. Существенным является то, что весь перечень указанных мероприятий обязательно должен планироваться и использоваться с учетом особенностей функционирования информационной системы предприятия.

Установление особого режима конфиденциальности.

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

Как правило, установление особого режима конфиденциальности включает в себя:

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

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

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

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

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

- организацию ремонта технических средств обработки конфиденциальной информации;

- организацию контроля за установленным порядком.

Условия соблюдения особого режима конфиденциальности

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

Ограничение доступа к конфиденциальной информации способствует созданию наиболее эффективных условий сохранности конфиденциальной информации. Необходимо четко определять круг сотрудников, допускаемых к конфиденциальной информации, к каким конкретно сведениям им разрешен доступ и полномочия сотрудников по доступу к конфиденциальной информации.

Традиционно для организации доступа к конфиденциальной информации использовались организационные меры, основанные на строгом соблюдении сотрудниками процедур допуска к информации, определяемых соответствующими инструкциями, приказами и другими нормативными документами.

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

Организация контроля за соблюдением установленного режима конфиденциальности.

Осуществление контроля за соблюдением установленного режима конфиденциальности предусматривает проверку соответствия организации защиты информации установленным требованиям, а также оценку эффективности применяемых мер защиты информации.

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

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

- вывод о соответствии проводимых на предприятии мероприятий установленным требованиям;

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

Необходимость создания органов защиты информации.

Для обеспечения и реализации перечисленных мероприятий (контроль, планирование и т.д.) потребуется создание соответствующих органов защиты информации. Эффективность защиты информации во многом будет определяться тем, насколько правильно выбрана структура органа защиты информации и квалифицированы его сотрудники.

Как правило, органы защиты информации представляют собой самостоятельные подразделения, однако на практике часто используется назначение одного из штатных специалистов организации, ответственным за обеспечение защиты информации.

Однако такая форма оправдана в тех случаях, когда объем необходимых мероприятий по защите информации небольшой и создание отдельного подразделения экономически не выгодно.

Средства защиты информации при передача ее по каналам связи.

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

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

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

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

2.2. Требования к организации управления ключевой информацией СКЗИ

Хранение ключевых носителей.

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

При наличии в организации, эксплуатирующей СКЗИ, ответственного пользователя СКЗИ (далее - администратора безопасности) и централизованном хранении ключевых носителей **администратор безопасности организации несет персональную ответственность за хранение личных ключевых носителей пользователей**. Личные ключевые носители администратора безопасности должны хранится в его личном сейфе.

Сроки действия ключей.

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

Сроки действия системной ключевой информации (например, выдающего центра системы управления сертификатами), как правило, не должны превышать 3-5 лет.

Уничтожение ключевой информации на ключевых носителях.

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

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

Учет пользовательской ключевой информации

В организации должен вестись "Журнал учета квалифицированных ключей", в которых следует вносить следующую информацию:

- Ф.И.О. лица, производящего запись;

- дата создания ключа;

- идентификаторы ключа (таблицы ключей) (например: серия, номер, комплект и т.п.);

- дата передачи/получения ключа;

- Ф.И.О. получателя/отправителя ключа;

- номер и дата акта о передаче ключа или подпись получателя;

- номер и дата акта об уничтожении ключа;

- запись о компрометации ключа.

Рекомендации по размещению технических средств СКЗИ.

При размещении технических средств СКЗИ, следует руководствоваться следующими рекомендациями:

1. Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства СКЗИ, посторонних лиц, по роду своей деятельности, не являющихся персоналом, допущенным к работе в этих помещениях.

2. Рекомендуется не использовать в помещении, где размещены рабочие места с установленным СКЗИ, радиотелефоны и другую радиоаппаратуру.

3. Должны выполняться требования политики безопасности, принятой в организации в области размещения технических средств, обрабатывающих конфиденциальную информацию.

Требования к программному и аппаратному обеспечению.

На технических средствах, оснащенных СКЗИ, должно использоваться только лицензионное программное обеспечение (далее по тексту – ПО), либо ПО, сертифицированное ФСБ России. Указанное ПО не должно содержать средств разработки и отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование СКЗИ. В любом случае ПО не должно содержать в себе возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;

- модифицировать код других подпрограмм;

- модифицировать память, выделенную для других подпрограмм;

- передавать управление в область собственных данных и данных других подпрограмм;

- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;

- использовать недокументированные фирмами разработчиками функции.

На ПЭВМ одновременно может быть установлена только одна разрешенная ОС.

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

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

Вход в BIOS ПЭВМ должен быть защищен паролем с длиной не менее б символов.

Организационные меры защиты информации от НСД.

При использовании СКЗИ должны соблюдаться следующие организационные меры:

1. Право доступа к рабочим местам с установленным ПО СКЗИ предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе СКЗИ.

2. Запрещается осуществление несанкционированного администратором безопасности копирование ключевых носителей.

3. Запрещается разглашение содержимого ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер.

4. Запрещается использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ, либо использовать ключевые носители на посторонних ПЭВМ.

5. Запрещается запись на ключевые носители посторонней информации.

6. На технических средствах, оснащенных СКЗИ, должно использоваться только лицензионное программное обеспечение фирм-производителей.

7. На ПЭВМ, оснащенных СКЗИ, не допускается установка средств разработки и отладки ПО. Если средства отладки приложений необходимы для технологических потребностей пользователя, то их использование должно быть санкционировано администратором безопасности. В любом случае запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений, использующих СКЗИ. Необходимо исключить попадание в систему программ, позволяющих, пользуясь ошибками ОС, получать привилегии администратора.

8. Должен быть исключен несанкционированный доступ посторонних лиц в помещения, в которых установлены технические средства СКЗИ, по роду своей деятельности, не являющихся персоналом, допущенным к работе в указанных помещениях.

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

10. Администратором безопасности должно быть проведено опечатывание системного блока с установленным СКЗИ, исключающее возможность несанкционированного изменения аппаратной части рабочей станции.

11. Из состава системы должно быть исключено все оборудование, которое может создавать угрозу безопасности ОС. Также избегают использования любых нестандартных

аппаратных средств, имеющих возможность влиять на нормальный ход работы компьютера или ОС.

12. При использовании СКЗИ на ПЭВМ, подключенных к общедоступным сетям связи, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых

операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей.

13. В BIOS ПЭВМ определяются установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске, должны быть: отключена загрузка с гибкого диска, привода CD-ROM, исключены прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Применение ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС, не допускается.

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

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

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

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

18. Должно производиться физическое затирание содержимого удаляемых файлов.

19. Должны быть реализованы организационно-технические меры защиты.

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

Правила безопасности функционирования рабочих мест со встроенной СКЗИ.

1. Личные ключевые носители пользователей рекомендуется хранить в сейфе.

2. Рабочие места, на которые установлены СКЗИ, должны быть аттестованы комиссией. Результаты работы комиссии отражаются в "Акте готовности к работе».

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

4. Должностные инструкции администратора безопасности (его заместителя) и ответственного исполнителя должны учитывать требования настоящих Правил.

5. Системные блоки ПЭВМ с установленным СКЗИ должны быть опечатаны специально выделенной для этих целей печатью. Наряду с этим допускается применение других дополнительных средств контроля за доступом к ПЭВМ.

6. Администратор безопасности должен периодически (не реже одного раза в два месяца) проводить контроль целостности и легальности установленных копий ПО на всех АРМ со встроенной СКЗИ с помощью программ контроля целостности.

7. В случае обнаружения "посторонних» (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией в составе представителей служб информационной безопасности организации - владельца сети и организации - абонента сети (пользователя), где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения.

8. Не допускается оставлять без контроля вычислительные средства, входящие в состав СКЗИ, при включенном питании и загруженном программном обеспечении СКЗИ. При кратковременном перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана производится с использованием пароля доступа.

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

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

11. На ПЭВМ должна быть установлена только одна ОС.

12. ПО, установленное на ПЭВМ, не должно иметь встроенных средств разработки и отладки программ.

13. Должны быть приняты меры по исключению вхождения пользователей в режим конфигурирования BIOS (например, с использованием парольной защиты).

14. Должна быть исключена возможность работы на ПЭВМ, если во время начальной загрузки не проходят встроенные тесты.

15. ПЭВМ, обеспечивающие удаленный вход пользователей из глобальной сети, (например RAS сервер) не должны использовать ПО СКЗИ.

16. Пароли, назначаемые пользователям, должны отвечать требованиям соответствующих инструкции и нормативных документов (ГТК, ЦБ РФ).

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

2.3. Криптография

Криптография в современном мире

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

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

Симметричные криптосистемы

Принцип работы симметричных криптосистем (правильнее в данном случае назвать их криптоалгоритмами), основан на использовании определенных операций с информацией на одной стороне или абсолютно одинаковых (в прямом и

обратном порядке) или с маленькими различиями (например с разными методами разделения ключа).

Блочные, потоковые и гибридные системы

Самое общепринятое деление криптоалгоритмов организовано по их методу обработки информации.

Блочные криптоалгоритмы

Делят сообщение целиком на отдельные блоки равной длины и производят операции с каждым блоком.

Потоковые криптоалгоритмы

Обрабатывают поток информации по мере его поступления. При этом поток не имеет начала или конца для криптосистемы.

Разновидности ключей

Еще одно деление криптоалгоритмов обычно основано на принципе использования ключа или ключей. При этом есть координальная разница между симметричным криптоалгоритмом и симметричным ключом. Симметричный ключ является всего лишь одним из вариантов реализации симметричного криптоалгоритма, хотя данный вариант является самым

распространенным, есть и другие реализации использования ключей. Мы рассмотрим самые часто встречающиеся.

Ключом в криптографии называется некая цифровая последовательность, файл или фраза, при помощи которой можно либо сразу произвести дешифрование (декриптование) шифрованного сообщения, либо, преобразовав ключ, произвести данное действие.

Разновидность симметричного ключа предполагает использование для процессов шифрования и расшифрования (дешифрования) одинакового ключа

Основной минус

Ключ не может быть передан по небезопасным каналам, поскольку является компрометирующим фактором безопасности.

Плюсы

Широкая реализация разновидностей решений и скорость криптопреобразования информации.

При использовании первичного и вторичного ключей подразумевают систему, при которой первичный ключ является шифрующим, а вторичный расшифровывающим. В этом случае во время шифрования закладывается некий фактор, который необходим, чтобы преобразовать первичный ключ во вторичный.

Разновидность первичного и вторичного ключей предполагает использование для процессов шифрования и расшифрования (дешифрования) двух разных ключей, причем второй может быть получен из первого при использовании того же фактора преобразования, который применялся при шифровании.

Основной минус

Фактор преобразования должен быть каким-то образом передан второму абоненту или вычислен им самостоятельно. Именно фактор преобразования является слабым местом данной разновидности криптосистемы.

Плюсы

Дополнительная безопасность путем разделения функций первичного и вторичного ключей. Передача первичного ключа по открытым каналам не несет прямой угрозы конфиденциальности сообщения.

При оценке криптоалгоритмов, обычно как основное качество, учитывают их возможность противостоянию взлому и криптоанализу.

Взлом–процесс прямого перебора ключей с целью найти тот, который сможет расшифровать шифрованное сообщение. При этом злоумышленник должен иметь шифрованное сообщение, знать алгоритм, с которым оно шифровано и иметь программные и аппаратные

ресурсы для запуска подбора ключа или пароля. При этом облегченным взломом называется взлом, когда злоумышленнику известен хотя бы один фактор относительно ключа (например длина ключа или пароля, какие в нем могут быть символы и тп).

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

Криптоанализ делят на линейный и дифференциальный.

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

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

Распространенные алгоритмы

AES (англ. Advanced Encryption Standard) -американский стандарт шифрования

ГОСТ 28147-89—отечественный стандарт шифрования данных

DES (англ. Data Encryption Standard) -стандарт шифрования данных в США до AES

3DES (Triple-DES, тройной DES)

RC6 (Шифр Ривеста)

Twofish

IDEA (англ.International Data Encryption Algorithm)

SEED - корейский стандарт шифрования данных

Camellia - сертифицированный для использовании в Японии шифр

CAST (по инициалам разработчиков Carlisle Adams и Stafford Tavares)

XTEA - наиболее простой в реализации алгоритм.

2.4. Электронная подпись

При постепенном переводе данных в электронный вид, встал вопрос не только о сохранении конфиденциальности документа (применением шифрования), целостности документа (применением хэширования), но также и привязке документа к человеку и однозначное отношение этого человека к документу. Эти требования к электронному документообороту носят название подтверждение авторства и невозможность отказа от авторства. Именно их реализует электронная подпись (далее – ЭП).

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

Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

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

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

Участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

Корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

Также можно сказать что ЭП - реквизит электронного документа, обеспечивающий сохранение авторства и неизменности документа при его пересылке и ознакомлении, а также (как дополнительная функция), возможность применения системы разграничения доступа к документу и его использования на уровне пользователей.

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

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

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

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

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

Первичная ЭП, которой заверяется и защищается от изменение содержимое самого сообщения. Первичная подпись может быть только одна.

Другие виды ЭП не могут находится в документе без первичной ЭП.

Дополняющая ЭП, которой дополнительно заверяется содержимое, но, например, другим пользователем или сертификатом. Дополняющая подпись существует только при наличии Первичной подписи, при этом доверие первичной подписи не обязательно. Дополняющая подпись может отсутствовать в документе, может быть одна или сразу несколько.

Заверяющая ЭП, которая заверяет не содержимое, а одну из подписей (Первичную или одну из дополняющей). При этом не обязательно доверие содержимому документа, но обязательно доверие к подписи, которая заверяется. Заверяющая подпись может отсутствовать, либо присутствовать на любом уровне, также заверяющих подписей может быть несколько.

В соответствии с 63-ФЗ существуют следующие виды электронных подписей простая электронная подпись и усиленная электронная подпись. Усиленная квалифицированная электронная подпись (далее - квалифицированная электронная подпись).

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

Неквалифицированной электронной подписью является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

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

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с 63-ФЗ.

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

Выделяются два формата ЭП:

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

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

В число дополнений входят:

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

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

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

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

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

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

2.5. Крипто Про CSP.

Крипто Про CSP реализует следующие алгоритмы

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

• ГОСТ Р 34.11-94–функция хэширования

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

Сертификат ФСБ РФ подтверждает, что реализованные алгоритмы и внутренние средства защиты СКЗИ Крипто Про CSP позволяют защищать с его помощью конфиденциальную информацию.

К средствам защиты государственной тайны предъявляются более высокие требования, поэтому средствами СКЗИ Крипто Про CSP **НЕ ДОПУСКАЕТСЯ** защищать информацию, составляющую государственную тайну.

Криптографические алгоритмы ГОСТ Р 34.11-94 (функция хэширования) и ГОСТ Р 34.10-2001 (ЭП), реализованные в СКЗИ Крипто Про CSP, а также сертификат ФСБ, позволяют использовать его в соответствии с требованиями 63-ФЗ как сертифицированное средство ЭП для авторизации, контроля целостности и обеспечения юридической значимости электронных документов.

Симметричное шифрование и имитозащита по ГОСТ 28147-89 позволяют использовать Крипто Про CSP для обеспечения конфиденциальности и контроля целостности информации.

По протоколу Диффи-Хеллмана на основе асимметричного алгоритма ГОСТ Р 34.10-2001 может быть создан общий секрет, что даёт возможность выработки общего ключа симметричного шифрования на основе асимметричных ключей с аутентификацией сторон. Эта функциональность позволяет реализовать протокол асимметричного шифрования с ключами ГОСТ Р 34.10-2001.

Крипто Про CSP поддерживает формат сертификатов открытых ключей X.509 и реализует все необходимые алгоритмы для установления защищённого соединения по протоколу TLS с аутентификацией одной или двух сторон.

Созданное таким образом соединение обеспечивает должный уровень защиты для передачи по каналу связи конфиденциальной информации.

Внутренние средства защиты Крипто Про CSP обеспечивают контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированного изменения или от нарушения правильности функционирования.

Это необходимо для обеспечения требуемого уровня защиты обрабатываемой информации и криптографических ключей.

Крипто Про CSP реализует процедуры управления криптографическими ключами, такие как создание, копирование и удаление. Таким образом, Крипто Про CSP может использоваться для управления ключевыми элементами системы в целях реализации регламента средств защиты.

Требуемый уровень защиты ключей обеспечивается только при работе с ними штатными средствами Крипто Про CSP. Например, удалять ключ путём форматирования дискеты нельзя.

Крипто Про CSP 3.6

• Текущая сертифицированная версия;

• Ключевые изменения по сравнению с 3.0: работа на Windows Vista/2008/W7, на процессорах x64, расширен перечень поддерживаемых UNIX-платформ;

• Поддерживается установка на КПК и смартфоны под управлением Windows Mobile.

Все версии Крипто Про CSP совместимы по форматам сообщений. Например, можно установить TLS-соединение с клиента версии 3.0 на сервер с версией 3.6. Аналогично, электронное письмо, зашифрованное и подписанное в версии 3.6 будет корректно расшифровано и проверено в версии 2.0.

Поддерживается обратная совместимость ключевых контейнеров. Ключи, созданные в более ранних версиях Крипто Про CSP могут использоваться в более поздних версиях, но не наоборот.

Размеры ключей электронной подписи:

• закрытый ключ –256 бит

• открытый ключ –512 бит

Размеры ключей, используемых при шифровании:

• закрытый ключ –256 бит

• открытый ключ –512 бит

• симметричный ключ –256 бит

Указанные размеры ключей определены соответствующими ГОСТами и не изменяются. Открытый ключ длиной 512 бит считается в настоящее время достаточным для асимметричных алгоритмов на эллиптических кривых, а размер закрытого ключа определяется размером

открытого ключа. Симметричный ключ размером 256 бит также считается достаточным для обеспечения высокого уровня защиты.

Симметричные ключи ГОСТ 28147-89 вырабатываются либо для одного сеанса связи, либо для защиты одного сообщения, и поэтому передаются и хранятся вместе с этим сообщением (обязательно в защищённом виде). Таким образом, хранение симметричных ключей на специальных носителях не требуется.

СКЗИ Крипто Про CSP может сохранять закрытые ключи ГОСТ Р 34.10-2001 на различных ключевых носителях. Ключ на ключевом носителе может быть защищён паролем. Поддерживаются следующие типы носителей:

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

• Смарт-карты и USB-токены;

• Идентификаторы (таблетки) Touch Memory;

• Жёсткий диск или реестр Windows.

Хранение ключевых носителей.

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

При наличии в организации, эксплуатирующей СКЗИ, администратора безопасности, и централизованном хранении ключевых носителей, администратор безопасности организации несет персональную ответственность за хранение личных ключевых носителей пользователей. Личные ключевые носители администратора безопасности должны храниться в его личном сейфе.

При хранении ключей на жёстком диске или в реестре Windows требования по хранению личных ключевых носителей распространяются на ПЭВМ. При использовании реестра требования сохраняются в том числе и после удаления ключей из реестра.

Настоятельно рекомендуется использовать парольную защиту при хранении ключей в реестре или на жёстком диске.

Сроки жизни ключей.

В руководстве по эксплуатации СКЗИ Крипто Про CSP установлены следующие сроки действия ключей:

• максимальный срок действия закрытых ключей шифрования и ЭП –1 год 3 месяца;

• максимальный срок действия открытых ключей шифрования –1 год 3 месяца;

• максимальный срок действия открытых ключей ЭП –30 лет.

После истечения установленных сроков действия закрытые ключи должны быть уничтожены во избежание неявной компрометации, а открытым ключам не следует доверять.

Обратите внимание на различие сроков действия, закрытого и открытого ключей ЭП. Для создания ЭП закрытый ключ может использоваться 1 год 3 месяца, после чего он должен быть уничтожен, но проверять созданные ЭП с помощью открытого ключа можно в течение 30 лет.

Срок действия открытого ключа дополнительно ограничивается сроком действия сертификата открытого ключа, который устанавливается в соответствии с регламентом выдавшего данный сертификат Удостоверяющего Центра.

План
обучения работников ТОГКУ «МФЦ» правилам работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну

№ п/п	Изучаемые вопросы (темы)	Кол-во часов	Форма (метод) подготовки	Лицо, ответственное за проведение мероприятия
1	2	3	4	5
1.	Организация защиты информации при использовании СКЗИ	4	Самоподготовка	
2.	Требования к организации управления ключевой информацией СКЗИ			
3.	Криптография			
4.	Электронная подпись			
5.	Крипто Про CSP			
6.	Работа на ПЭВМ с ОС «Windows» и офисными приложениями; работа с базами данных. Порядок применения СКЗИ.	4	Практическое занятие	Администратор безопасности
7.	Порядок представления конфиденциальных данных в электронном виде по телекоммуникационным каналам связи с помощью АИС МФЦ и ПК ПВД в рамках организации предоставления государственных и муниципальных услуг в МФЦ по принципу «одного окна»	2	Практическое занятие	Администратор безопасности

Приложение № 5
к Положению об организации и проведении работ
по обеспечению безопасности конфиденциальной информации
с использованием средств криптографической защиты в ТОГКУ «МФЦ»

Журнал
учета обучения пользователей средств криптографической защиты информации

№ п/п	Должность	Ф.И.О. пользователя СКЗИ	Номер и дата приказа о назначении	Программа обучения	Период проведения обучения	Подпись обучаемого по итогам обучения, дата	Подпись лица, проводившего обучение, дата
1	2	3	4	5	6	7	8

ПРИЛОЖЕНИЕ № 2
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от 20.12.2017 г. № 81.1-од

Инструкция
ответственного пользователя средств криптографической защиты информации в информационной системе Тамбовского областного государственного казенного учреждения «Многофункциональный центр предоставления государственных и муниципальных услуг»

1. Общие положения

1.1. Настоящая Инструкция ответственного пользователя средств криптографической защиты информации в информационной системеТамбовского областного государственного казенного учреждения«Многофункциональный центр предоставления государственных и муниципальных услуг» (далее – Инструкция) разработана в соответствии с требованиями приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.2. Настоящая Инструкция определяет общие функции, права и обязанности ответственного пользователя средств криптографической защиты информации в информационной системе Тамбовского областного государственного казенного учреждения«Многофункциональный центр предоставления государственных и муниципальных услуг» (далее – Ответственный пользователь криптосредств) при исполнении им своих функциональных обязанностей по обеспечению функционирования и безопасности средств криптографической защиты (далее – криптосредств).

1.3. Ответственный пользователь криптосредств в своей деятельности руководствуется организационно-распорядительной документацией, определяющей политику информационной безопасности и ее реализацию при эксплуатации ИС в Тамбовском областном государственном казенном учреждении«Многофункциональный центр предоставления государственных и муниципальных услуг» (далее – ТОГКУ «МФЦ»), Положением об организации и проведении работ по обеспечению безопасности конфиденциальной информации с использованием средств криптографической защиты в ТОГКУ «МФЦ», а также другими документами, регламентирующими защиту конфиденциальной информации, в том числе персональных данных.

1.4. Назначение на должность Ответственного пользователя криптосредств и освобождение от нее производится приказом директора ТОГКУ «МФЦ».

1.5. На время отсутствия Ответственного пользователя криптосредств его обязанности исполняет другой специалист, с которым предварительно проводится инструктаж по обслуживанию криптосредств в ТОГКУ «МФЦ». Назначенный сотрудник приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

1.6. Ответственный пользователь криптосредств, а также лицо, его замещающее, должны быть ознакомлены под подпись с настоящей Инструкцией.

1.7. Настоящая Инструкция разработана на основании действующих нормативных документов по вопросам защиты конфиденциальной информации с использованием криптосредств.

2. Обязанности Ответственного пользователя криптосредств

2.1. Выполнять требования, указанные в технической документации, поставляемой вместе со средствами криптографической защиты информации.

2.2. Вести поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним, носителей конфиденциальных данных в «Журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов» с использованием индексов или условных наименований и регистрационных номеров.

2.3. Вести учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности конфиденциальных данных в информационной системе (далее – пользователи криптосредств) в «Журнале учета пользователей криптосредств», форма которого приведена в Приложении 1 к данной Инструкции.

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

2.5. Производить установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к этим средствам. Установка криптосредств оформляется актом, форма которого приведена в Приложении 2 к данной Инструкции.

2.6. Проверять готовность криптосредств к использованию с составлением заключений о возможности их эксплуатации.

2.7. Проводить обучение лиц, использующих криптосредства, работе с ними.

2.8. Осуществлять контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним, обеспечением функционирования и безопасности криптосредств.

2.9. Выполнять указания ответственного за обеспечение безопасности персональных данных в информационной системеТОГКУ «МФЦ» по вопросам осуществления взаимодействия операторов информационных систем при использовании

криптосредств для обеспечения безопасности обработки персональных данных для организации взаимодействия криптосредств.

2.10. Немедленно вывести из действия криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

2.11. Принимать срочные меры к розыску ключевых документов в случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения.

2.12. Устанавливать, по согласованию с руководством, режим охраны помещений, в которых установлены криптосредства или хранятся ключевые документы к ним, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время.

2.13. Проводить периодический контроль за выполнением установленного режима охраны помещений, в которых установлены криптосредства или хранятся ключевые документы к ним, состояния технических средств охраны, если таковые имеются.

2.14. Хранить в сейфе дубликаты ключей от входных дверей помещений, в которых установлены криптосредства или хранятся ключевые документы к ним.

2.15. Хранить в сейфе дубликаты ключей от хранилищ пользователей криптосредств, в случае хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей в хранилищах пользователей криптосредств.

2.16. Устанавливать порядок хранения ключевых и других документов в хранилище пользователя криптосредств, при утрате ключа от хранилища или от входной двери в помещение, в котором установлены криптосредства или хранятся ключевые документы к ним, до изменения секрета замка.

2.17. Оценивать возможность компрометации хранящихся ключевых и других документов, составлять акт и принимать при необходимости меры к локализации последствий компрометации конфиденциальных данных и к замене скомпрометированных криптоключей, в случае обнаружения признаков, указывающих на возможное несанкционированное проникновение в помещения или хранилища, в которых установлены криптосредства или хранятся ключевые документы к ним, посторонних лиц.

2.18. Не разглашать информацию, к которой он допущен, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты.

2.19. Соблюдать требования к обеспечению безопасности конфиденциальных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

2.20. Сообщать о ставших ему известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним директору ТОГКУ «МФЦ».

2.21. Немедленно уведомлять ответственного за обеспечение безопасности персональных данных в информационной системеТОГКУ «МФЦ» о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых конфиденциальных данных.

2.22. Сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным в документе «Состав и содержание организационных и технических мер…», утвержденном приказом ФСБ России от 10.07.2014 № 378, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

2.23. Выполнять положения, предусмотренные документом «Состав и содержание организационных и технических мер…», утвержденным приказом ФСБ России от 10.07.2014 №378, и настоящей Инструкцией, в полном объеме.

3. Права Ответственного пользователя криптосредств

3.1. Инициировать разбирательство и составление заключений по фактам нарушения условий хранения носителей конфиденциальных данных, использования криптосредств, которые могут привести к нарушению конфиденциальности данных или другим нарушениям, приводящим к снижению уровня защищенности конфиденциальных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений в соответствии с «Положением о порядке организации и проведения работ по обеспечению безопасности персональных данных в информационной системеТОГКУ «МФЦ».

3.2. Санкционировать передачу криптосредств, эксплуатационной и технической документации к ним, ключевых документов между пользователями криптосредств под расписку в «Журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов».

3.3. Принимать неиспользованные или выведенные из действия ключевые документы от пользователей криптосредств, давать указания по уничтожению ключевых документов на месте.

3.4. Уничтожать ключевые документы под расписку в «Журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов».

3.5. Требовать от пользователей криптосредств уведомления об уничтожении пользователями криптоключей, использованных непосредственно ими (предназначенных для них).

3.6. Принимать решение об использовании скомпрометированных криптоключей при условии максимально короткого периода их использования, в чрезвычайных случаях,

когда отсутствуют криптоключи для замены скомпрометированных, по согласованию с руководством.

3.7. Вскрывать помещения, в которых установлены криптосредства или хранятся ключевые документы к ним, и хранилища пользователей криптосредств.

4. Ответственность, возлагаемая на Ответственного пользователя криптосредств

4.1. Ответственный пользователь криптосредств несет ответственность за:

– несоблюдение требований документов, регламентирующих организацию и обеспечение функционирования и безопасности криптосредств, предназначенных для защиты конфиденциальных данных при их обработке в информационных системах, в соответствии с действующим законодательством Российской Федерации;

– выполнение мероприятий по текущему контролю за организацией и обеспечением функционирования криптосредств;

– правильность и объективность принимаемых решений;

– правильное и своевременное выполнение приказов, распоряжений, указаний руководства ТОГКУ «МФЦ» по вопросам работы с криптосредствами;

– выполнение возложенных на него функциональных обязанностей;

– разглашение сведений ограниченного распространения, ставших известными ему в ходе выполнения служебных обязанностей;

– соблюдение трудовой дисциплины, охраны труда;

– качество проводимых работ по организации и контролю за соблюдением требований, установленных законодательством Российской Федерации в области защиты конфиденциальной информации.

5. Заключение

5.1. Настоящая Инструкция доводится до ответственного пользователя средств криптографической защиты информации в информационной системе ТОГКУ «МФЦ» под роспись.

5.2. Настоящая Инструкция вступает в силу с момента её утверждения.

Приложение№1
к Инструкции ответственного пользователя средств
криптографической защиты информации
в информационной системе в ТОГКУ «МФЦ

Журнал
учета пользователей криптосредств

№№ ПП	Ф.И.О. пользователя	Серийный номер лицензии	Номер дистрибутива	Примечание
1	**2**	**3**	**4**	**5**
1.				
2.				
3.				
4.				

Приложение№2
к Инструкции ответственного пользователя средств
криптографической защиты информации
в информационной системе в ТОГКУ «МФЦ

УТВЕРЖДАЮ
Директор ТОГКУ «МФЦ»

М.П. _____ **Л.П. Третьякова**
«__»_____20__г.

Акт
установки средств криптографической защиты информации, ввода
в эксплуатацию и закрепления их за ответственными лицами

_____ _____
(наименование населенного пункта) (дата, месяц, год)

Настоящий акт составлен о том, что _____ сотрудником
(дата)
_____
(наименование организации, должность, фамилия, имя, отчество, иные сведения (например, дата, номер лицензии))

(далее – Администратор ИБ) была произведена установка и настройка средства криптографической защиты информации _____
(наименование)
далее - СКЗИ на ПЭВМ (АРМ Заявителя):
Серийный № (Инв. №) ПЭВМ _____

Место установки _____
_____
(адрес местонахождения, номер помещения)
Ф.И.О. пользователя АРМ Заявителя ____
_____
(должность, фамилия, имя, отчество)
(далее - пользователь СКЗИ) _____

Рег. № СКЗИ (номер экземпляра) _____
№ дистрибутива _____

Размещение АРМ Заявителя, хранение ключевых носителей, охрана помещений организованы установленным порядком;

Обучение правилам работы с СКЗИ и проверка знаний нормативно правовых актов и эксплуатационной и технической документации к ним проведены.

Условия для использования СКЗИ, установленные эксплуатационной и технической документацией к СКЗИ созданы

Установленное и настроенное СКЗИ находится в работоспособном состоянии.

Формуляр и дистрибутив на носителе находится на ответственном хранение у ответственного пользователя СКЗИ _____.

Пользователь АРМ Заявителя обязуется:

- не разглашать конфиденциальную информацию, к которой он допущен, в том числе криптоключи и сведения о ключевой информации;

- соблюдать требования к обеспечению безопасности СКЗИ и ключевых документов к ним;

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

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

	/	/
(должность Администратора ИБ)	*(подпись)*	*(Фамилия И.О.)*
	/	/
(должность ответственного лица пользователя АРМ заявителя)	*(подпись)*	*(Фамилия И.О.)*

ПРИЛОЖЕНИЕ № 3
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от 20.12.2017 г. № 81.1-од

Инструкция

по применению криптографических средств для защиты конфиденциальной информации в информационных системах Тамбовского областного государственного казенного учреждения «Многофункциональный центр предоставления государственных и муниципальных услуг»

1. Общие положения

1.1.Настоящая Инструкция по применению криптографических средств для защиты конфиденциальной информации в информационных системах Тамбовского областного государственного казенного учреждения«Многофункциональный центр предоставления государственных и муниципальных услуг» (далее – Инструкция) разработана в соответствии с требованиями приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.2.Настоящая Инструкция определяет права и обязанности пользователя шифровальных (криптографических) средств (далее – пользователь криптосредств), предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну (далее – криптосредство), в информационной системе Тамбовского областного государственного казенного учреждения«Многофункциональный центр предоставления государственных и муниципальных услуг» (далее – ТОГКУ «МФЦ»).

1.3.На пользователя криптосредств возлагаются обязанности по соблюдению сохранности криптосредств, ключевой, эксплуатационной и технической документации и выполнению требований по вопросам работы с криптосредствами.

1.4.Пользователь криптосредств допускается к работе с ними по решению директора ТОГКУ «МФЦ».

2. Права пользователя криптосредств

Пользователь криптосредств имеет право:

– использовать в работе для выполнения служебных обязанностей криптосредства;

– хранить инсталлирующие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования;

– передавать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку в «Журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов» при согласовании с ответственным пользователем криптосредств;

– принимать меры по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.;

– уничтожать неиспользованные или выведенные из действия ключевые документы, использованные непосредственно им (предназначенные для него), по указанию ответственного пользователя криптосредств.

3. Обязанности пользователя криптосредств

Пользователь криптосредств обязан:

– не разглашать информацию о ключевых документах;

– не допускать снятие копий с ключевых документов;

– не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;

– не допускать записи на ключевой носитель посторонней информации;

– не допускать установки ключевых документов в другие ПЭВМ;

– соблюдать конфиденциальность при обращении со сведениями, которые ему доверены или стали известны в работе, в том числе со сведениями о криптосредствах, ключевых документах к ним, о функционировании и порядке обеспечения безопасности применяемых криптосредств и ключевых документах к ним;

– соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;

– хранить инсталлирующие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы, носители информации ограниченного распространения в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение;

– предусматривать раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае

компрометации действующих ключевых документов;

– передавать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы только между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета;

– передавать служебные сообщения ограниченного доступа, касающиеся организации и обеспечения функционирования криптосредств, по техническим средствам связи только с использованием криптосредств;

– не допускать передачи по техническим средствам связи криптоключей;

– сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

– немедленно уведомлять ответственного пользователя криптосредств о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных;

– сообщать ответственному пользователю криптосредств о нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием персональных данных;

– возвращать ответственному пользователю криптосредств неиспользованные или выведенные из действия ключевые документы или по его указанию уничтожать на месте;

– уведомить об уничтожении ключевых документов, использованных непосредственно им (предназначенных для него), ответственного пользователя криптосредств;

– выполнять указания ответственного за обеспечение безопасности персональных данных в информационной системе ТОГКУ «МФЦ» по вопросам осуществления взаимодействия операторов информационных систем при использовании криптосредств для обеспечения безопасности обработки персональных данных для организации взаимодействия криптосредств;

– сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным приказом ФСБ России от 10.07.2014 № 378, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

4. Ответственность пользователя криптосредств

Пользователь криптосредств несет ответственность за:

– несоблюдение требований документов, регламентирующих организацию и обеспечение функционирования и безопасности криптосредств, предназначенных для защиты персональных данных при их обработке в информационной системе, в соответствии с действующим законодательством Российской Федерации;

– правильность и объективность принимаемых решений;

– сохранность криптосредств, ключевой, эксплуатационной и технической документации, носителей информации ограниченного распространения, а также за порученные участки работы;

– выполнение требований к обеспечению безопасности персональных данных;

– правильное и своевременное выполнение приказов, распоряжений, указаний руководства по вопросам работы с криптосредствами в ТОГКУ «МФЦ»;

– выполнение возложенных на него обязанностей, предусмотренных настоящей Инструкцией;

– разглашение сведений ограниченного распространения, ставших известными ему в ходе выполнения служебных обязанностей;

– соблюдение правил внутреннего трудового распорядка, трудовой дисциплины, охраны труда.

5. Порядок действий при компрометации криптоключей

Под компрометацией криптоключей понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам. К компрометации ключей относятся следующие события:

− утрата носителей ключа;

− утрата иных носителей ключа с последующим обнаружением;

− увольнение сотрудников, имевших доступ к ключевой информации;

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

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

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

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

− доступ посторонних лиц к ключевой информации;

− другие события утери доверия к ключевой документации.

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

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать руководству.

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.

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

При наступлении любого из перечисленных выше событий пользователь должен немедленно прекратить связь с другими пользователями и сообщить о факте компрометации (или предполагаемом факте компрометации) Администратору безопасности.

Расследование факта компрометации (или предполагаемой компрометации) должно проводиться на месте происшествия специально назначаемой комиссией во главе с Администратором безопасности.

Результатом рассмотрения является квалификация или не квалификация данного события как компрометация действующих ключей.

При установлении факта компрометации действующих ключей, скомпрометированные секретные ключи шифрования и подписи уничтожаются.

Для восстановления конфиденциальной связи после компрометации ключей пользователь обращается к Администратору безопасности с целью регистрации вновь изготовленных (или резервных) ключей. Регистрация новых ключей шифрования и ЭЦП осуществляется тем же порядком, как и при плановой смене ключей.

6. Заключение

6.1.Настоящая Инструкция по применению криптографических средств для защиты конфиденциальной информации в информационных системах ТОГКУ «МФЦ» доводится до пользователей криптосредств под роспись.

6.2.Настоящая Инструкция вступает в силу с момента её утверждения.

ПРИЛОЖЕНИЕ № 4
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от 20.12.2017 г. № 81.1-од

Порядок

доступа в помещения Тамбовского областного государственного казенного учреждения «Многофункциональный центр предоставления государственных и муниципальных услуг», в которых ведется обработка персональных данных

1. Общие положения

1.1.Настоящий Порядок доступа в помещения Тамбовского областного государственного казенного учреждения «Многофункциональный центр предоставления государственных и муниципальных услуг», в которых ведется обработка персональных данных (далее – Порядок), разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), частью 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденного постановлением Правительства РФ от 21 марта 2012 г. № 211, постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также Приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.2.Целью настоящего Порядка является обеспечение безопасности персональных данных при их обработке (в том числе хранении) путем создания условий, затрудняющих несанкционированный доступ к техническим средствам и средствам защиты, участвующим в обработке персональных данных, и машинным носителям персональных данных.

1.3.Ознакомлению с настоящим Порядком подлежат все лица, имеющие право доступа и самостоятельного пребывания в помещениях Тамбовского областного государственного казенного учреждения «Многофункциональный центр предоставления государственных и муниципальных услуг» (далее – ТОГКУ «МФЦ»), в которых установлены технические средства автоматизированной системы ТОГКУ «МФЦ», размещены используемые средства защиты информации, в том числе средства криптографической защиты информации (далее – СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ или хранятся машинные носители персональных данных (далее – Помещения).

1.4.Настоящий Порядок вступает в силу с момента его утверждения и действует до его отмены либо замены новым Порядком.

2. Требования к помещениям

2.1.Для помещений, в которых установлены технические средства автоматизированной системы ТОГКУ «МФЦ», а также хранятся и обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащей персональные данные, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Данный режим достигается:

– оснащением помещения входными дверьми с замками;

– обязательным запиранием помещения на ключ, даже при выходе из него в рабочее время;

– отдельным хранением дубликатов ключей;

– закрытием металлических шкафов и сейфов, где хранятся носители информации, содержащие персональные данные;

– утверждением перечня лиц, имеющих право доступа в помещение.

Сейфы (металлические шкафы) для хранения съемных машинных носителей персональных данных должны быть оборудованы внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

2.2.Для помещений, в которых размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации

СКЗИ, организуется режим обеспечения безопасности, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения. Данный режим достигается:

– оснащением помещения входными дверьми с замками;

– обеспечением постоянного закрытия дверей Помещения на замок и их открытия только для санкционированного прохода;

– опечатыванием помещения по окончании рабочего дня или оборудованием помещения соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещения;

– отдельным хранением дубликатов ключей;

– закрытием металлических шкафов и сейфов, где хранятся носители ключевой, аутентифицирующей и парольной информации СКЗИ;

– утверждением перечня лиц, имеющих право доступа в Помещения.

Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей должно быть предусмотрено необходимое число надёжных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у ответственного за организацию обработки персональных данных в ТОГКУ «МФЦ».

По окончании рабочего дня установленные в помещении хранилища должны быть опечатаны. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей СКЗИ, ответственных за эти хранилища.

При утрате ключа от хранилища или от входной двери в помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный за организацию обработки персональных данных в ТОГКУ «МФЦ».

3. Организация доступа в Помещения

3.1.В Помещения допускаются сотрудники ТОГКУ «МФЦ», указанные в «Перечне лиц, имеющих право самостоятельного доступа в помещения, в которых

располагаются информационные системы ТОГКУ «МФЦ» (далее – Перечень), утвержденном приказом директора ТОГКУ «МФЦ».

3.2.Помимо лиц, указанных в Перечне (далее – лица, имеющие право доступа в Помещения), право самостоятельного пребывания в Помещениях, для которых введен режим безопасности, имеет директор ТОГКУ «МФЦ».

3.3.Лица, не внесенные в Перечень (далее – лица, не имеющие право доступа в Помещения), являются сторонними лицами и могут находиться в Помещениях только в присутствии лиц, имеющих права доступа в Помещения.

3.4.Посторонние лица имеют право пребывать в Помещениях только в присутствии лиц, имеющих право доступа в Помещения, и в течение ограниченного количества времени, необходимого для решения вопросов, связанных с исполнением государственных (муниципальных) функций и (или) осуществлением полномочий в рамках договоров, заключенных с Организацией, обслуживанием компьютерной техники и оргтехники.

3.5.Доступ в Помещения разрешается только в рабочее время.

3.6.В течение рабочего времени лица, имеющие право доступа в Помещения:

– закрывают дверь Помещения на ключ при оставлении последним Помещения (при этом запрещается оставлять ключ в замке Помещения);

– не покидают Помещение, если в нем находятся лица, не имеющие право доступа в Помещения;

– при обнаружении фактов нарушения режима безопасности Помещения ставят в известность ответственного за обеспечение безопасности персональных данных в информационной системеТОГКУ «МФЦ» (далее – Ответственный за обеспечение безопасности ПДн);

– при посещении Помещения посторонними лицами с целями проведения контрольных, проверочных мероприятий, а также работ по обслуживанию Помещения и его инженерно-технических средств ставят в известность Ответственного за обеспечение безопасности ПДн и директора ТОГКУ «МФЦ».

3.7.Доступ в Помещения в нерабочее время возможен только по письменной заявке работника, согласованной с директором ТОГКУ «МФЦ» и имеющей разрешающую резолюцию. Данные заявки хранятся у Ответственного за обеспечение безопасности ПДн.

3.8. Доступ в Помещения при возникновении нештатной ситуации в нерабочее время осуществляется в присутствии Ответственного за обеспечение безопасности ПДн с составлением акта на вскрытие (далее – акт).

В акте необходимо указать:

– фамилии, имена, отчества должностных лиц, принимавших участие во вскрытии Помещения;

– дату и время вскрытия Помещения;

– причины вскрытия Помещения;

– кто был допущен (должность и фамилия) в Помещение для ликвидации последствий нештатной ситуации;

– как осуществлялась охрана вскрытого Помещения в этот период;

– какое имущество, в каком количестве, куда эвакуировано из вскрытого Помещения и как осуществлялась его охрана;

– кто из должностных лиц и когда был информирован по указанному факту происшествия;

– другие сведения.

Акт подписывается должностными лицами, вскрывшими Помещение.

Вскрытие сейфов с машинными носителями, содержащими персональные данные, осуществляется работниками, отвечающими за их сохранность.

3.9. При обслуживании Помещений (уборка или ремонт Помещений, инженерно-технического оборудования):

– обслуживающий персонал находится в Помещении только в присутствии лиц, имеющих право доступа в Помещение;

– ключи от замков дверей Помещения обслуживающему персоналу и другим лицам, не имеющим права доступа в Помещение, без согласования с Ответственным за обеспечение безопасности ПДн не выдаются;

– сотрудники, обеспечивающие контроль действий обслуживающего персонала в Помещении, обязаны не допускать несанкционированных действий в отношении компонентов информационной системы и машинных носителей персональных данных;

– капитальный или иной ремонт может проводиться без присутствия лиц, имеющих право доступа в Помещение, только в том случае, если компоненты информационной системы и машинные носители персональных данных были предварительно вынесены из ремонтируемого Помещения в другое контролируемое Помещение, а по окончании ремонта заменены замки. Организует и контролирует исполнение Ответственный за обеспечение безопасности ПДн.

3.10.Лица, имеющие право доступа в Помещения, несут ответственность за нерегламентированное пребывание в Помещениях работников ТОГКУ «МФЦ» и иных сторонних лиц, не имеющих права доступа в Помещения.

4. Контроль соблюдения порядка доступа в Помещения

4.1.Контроль выполнения требований настоящего Порядка осуществляется Ответственным за обеспечение безопасности ПДн.

4.2.Ответственный за обеспечение безопасности ПДн в случае установления факта нарушения лицом, имеющим право доступа в Помещения, настоящего Порядка проводит с ним разъяснительную работу, а в случае неоднократного нарушения уведомляет директора ТОГКУ «МФЦ».

ПРИЛОЖЕНИЕ № 5
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от 20.12.2017 г. № 81.1-од

Список лиц,

допущенных к вскрытию и закрытию служебных помещений Тамбовского областного государственного казенного учреждения «Многофункциональный центр предоставления государственных и муниципальных услуг», где установлены средства криптографической защиты информации или хранятся ключевые документы к ним

№ п/п	Фамилия, имя, отчество	Должность	Помещение
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			

ПРИЛОЖЕНИЕ № 6
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
от 20.12.2017 г. № 81.1-од

Инструкция
о порядке действий при компрометации криптоключей

1. **Общие положения.**

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

К компрометации ключей относятся следующие события:

- утрата носителей ключа;
- утрата иных носителей ключа с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
- доступ посторонних лиц к ключевой информации;
- другие события утери доверия к ключевой документации.

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

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать руководству.

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.

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

Порядок работы пользователей СКЗИ устанавливается инструкцией пользователю СКЗИ, утвержденную приказом директора ТОГКУ «МФЦ».

На случай компрометации ключевых документов совместно с ними выдается «Карточка оповещения о компрометации», в которой указывается порядок действий пользователя, номера телефонов и другие способы связи, пароль, означающий факт компрометации криптоключей конкретного пользователя.

Действующие и резервные ключевые документы, предназначенные для применения в случае компрометации действующих криптоключей, должны храниться во внутреннем отсеке сейфа в различных конвертах.

2. Порядок действий пользователя при компрометации ключей

Первые пять событий должны трактоваться как безусловная компрометация действующих ключей; при наличии остальных событий требуется специальное расследование в каждом конкретном случае.

При наступлении любого из перечисленных выше событий пользователь должен немедленно прекратить связь с другими пользователями и сообщить о факте компрометации (или предполагаемом факте компрометации) Администратору безопасности.

Расследование факта компрометации (или предполагаемой компрометации) должно проводиться на месте происшествия специально назначаемой комиссией во главе с Администратором безопасности.

Результатом рассмотрения является квалификация или не квалификация данного события как компрометация действующих ключей.

При установлении факта компрометации действующих ключей, скомпрометированные секретные ключи шифрования и подписи уничтожаются.

Для восстановления конфиденциальной связи после компрометации ключей пользователь обращается к Администратору безопасности с целью регистрации вновь изготовленных (или резервных) ключей. Регистрация новых ключей шифрования и ЭЦП осуществляется тем же порядком, как и при плановой смене ключей.

ПРИЛОЖЕНИЕ № 7
УТВЕРЖДЕНО
приказом ТОГКУ «МФЦ»
20.12.2017 г. № 81.1-од

Состав
комиссии по допуску пользователей к самостоятельной работе с СКЗИ

Председатель комиссии:

- заместитель директора Небогин Александр Михайлович

Члены комиссии:

- начальник отдела ИТО Буздин Николай Викторович
- инженер программист отдела ИТО Кондеев Евгений Игоревич
- юрисконсульт отдела МТО Рябов Сергей Андреевич

ЛИСТ ОЗНАКОМЛЕНИЯ

с Инструкцией

о порядке действий при компрометации криптоключей

№ п/п	Дата	Должность	Фамилия, имя, отчество	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				
27.				
28.				
29.				
30.				