Методические рекомендации

по организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну

письмо заместителя Губернатора Смоленской области - председателя Комиссии по информационной безопасности при Администрации Смоленской области от 21 августа 2017 г. № 04/690

г. Смоленск 2017 г.

Настоящие рекомендации разработаны в соответствии с действующим законодательством в области обеспечения защиты информации средствами криптографической защиты информации.

Данные рекомендации предназначены для государственных и муниципальных служащих, занимающихся организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, а также лиц ответственных за эксплуатацию СКЗИ.

Методическими рекомендациями необходимо руководствоваться в следующих случаях:

– при определении порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну;

– при обеспечении с использованием криптосредств безопасности персональных данных при их обработке в государственных информационных системах персональных данных;

– при использовании криптосредств для обеспечения безопасности персональных данных в случаях, предусмотренных п.3 положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (ПКЗ-2005).

Методические рекомендации разработаны Управлением информационной безопасности смоленского областного государственного автономного учреждения «Центр информационных технологий».

Содержание

Список сокращений

ОКЗИ – орган криптографической защиты информации удостоверяющего центра смоленского областного государственного автономного учреждения «Центр информационных технологий»

ПЭВМ – персональная электронно-вычислительная машина

СКЗИ – средства криптографической защиты информации

1. Порядок обращения с СКЗИ и ключевыми документами

1.1. В организации, уполномоченные лица которой планируют в своей работе использовать СКЗИ, нормативным правовым актом руководителя назначается специалист, ответственный за эксплуатацию СКЗИ (Приложение № 2). Назначение специалиста допускается после прохождения им предварительной специальной подготовки (обучения). Ответственный за эксплуатацию СКЗИ в своей работе руководствуется положениями инструкции (Приложение № 3).

1.2. Обучение ответственного за эксплуатацию СКЗИ проводит ОКЗИ или специализированная организация, осуществляющая образовательную деятельность по данному направлению.

1.3. Выдача СКЗИ, эксплуатационной и технической документации к ним, ответственному за эксплуатацию СКЗИ осуществляется ОКЗИ.

1.4. СКЗИ, эксплуатационная и техническая документация к ним доставляются при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

1.5. Поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведется в соответствующих журналах.

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

1.7. Непосредственно к работе с СКЗИ допускаются пользователи, прошедшие соответствующую подготовку (обучение). Обучение пользователей правилам работы с СКЗИ организуется и проводится специалистом, ответственным за эксплуатацию СКЗИ. Учет проведения обучения пользователей СКЗИ ведется в соответствующем журнале.

1.8. Выдачу СКЗИ, эксплуатационной и технической документации к ним пользователям СКЗИ осуществляет ответственный за эксплуатацию СКЗИ, под расписку в журнале поэкземплярного учета. Пользователи СКЗИ несут персональную ответственность за сохранность полученных СКЗИ.

1.9. Пользователи СКЗИ хранят ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

1.10. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

1.11. Уничтожение ключевой информации и ключевых документов производится специалистом ОКЗИ, в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ. По факту уничтожения составляется акт об уничтожении криптографических ключей и ключевых документов, с отметкой об уничтожении в соответствующем журнале. Акт передается ответственному за эксплуатацию СКЗИ.

1.12. Криптоключи, в отношении которых возникло подозрение в компрометации, немедленно выводятся из действия. О выводе криптоключей из действия сообщается в ОКЗИ по телефону. В этот же день в ОКЗИ представляется письменное сообщение о компрометации криптоключей.

2. Порядок допуска пользователей к самостоятельной работе с СКЗИ

2.1. К самостоятельной работе с СКЗИ допускаются пользователи:

– назначенные на должности, выполнение обязанностей по которым связано с хранением и использованием СКЗИ;

– прошедшие специальную подготовку (обучение) по программе, утвержденной ОКЗИ или прошедшие повышение квалификации в специализированной организации, осуществляющей образовательную деятельность по данному направлению;

– успешно сдавшие зачет комиссии, на допуск к самостоятельной работе с СКЗИ.

2.2. Документом, подтверждающим специальную подготовку (обучение) пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение (Приложение № 5), составленное комиссией ОКЗИ на основании принятого зачета по программе подготовки (обучения) или документ, подтверждающий повышение квалификации по направлению СКЗИ. Заключения о допуске пользователей к самостоятельной работе с СКЗИ утверждаются руководителем организации.

2.3. Программа подготовки (обучения) пользователей к самостоятельной работе с СКЗИ (Приложение № 14) разработана ОКЗИ и включает:

– 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, правила применения и использовании электронной подписи в электронных документах, а также информацию об 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 и информационного обмена с использованием СКЗИ;

– изучение должностных инструкций, положений, других локальных нормативных актов по вопросам деятельности, связанной с разработкой, производством, хранением, реализацией и использованием СКЗИ;

– изучение эксплуатационно-технической документации на СКЗИ;

– приобретение практических навыков выполнения работ, предусмотренных обязанностями по занимаемой должности.

2.4. Методика подготовки пользователей к сдаче зачета на допуск к самостоятельной работе с СКЗИ определяется ответственным за эксплуатацию СКЗИ и предусматривает как формы самостоятельного изучения и освоения программного материала пользователем, так и формы группового и индивидуального обучения привлечением подготовленных специалистов в качестве преподавателей.

2.5. Ответственный за эксплуатацию СКЗИ может самостоятельно проводить специальную подготовку (обучение) пользователей по программе, утвержденной ОКЗИ, принимать зачёты и на их основании готовить заключение о возможности допуска пользователей к самостоятельной работе с СКЗИ.

2.6. Ответственность за полноту и качество подготовки пользователей к самостоятельной работе с СКЗИ несет ответственный за эксплуатацию СКЗИ.

3. Размещение, специальное оборудование, охрана и организация режима в помещениях, в которых установлены СКЗИ или хранятся ключевые документы

3.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы (далее - спецпомещения), должны исключать возможность неконтролируемого доступа и использования СКЗИ посторонними лицами, а также просмотра посторонними лицами ведущихся там работ.

3.2. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

3.3. Окна спецпомещений, расположенных на первых и последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, должны быть оборудованы металлическими решетками или охранной сигнализацией.

3.4. В спецпомещениях для хранения ключевых документов пользователям СКЗИ необходимо иметь надежно запираемые шкафы индивидуального пользования, оборудованные приспособлениями для опечатывания замочных скважин. Ключи от шкафов должны находиться у соответствующих Пользователей СКЗИ. Опечатанные шкафы пользователей СКЗИ могут быть вскрыты только самими пользователями.

3.5. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в индивидуальные шкафы пользователей СКЗИ посторонних лиц, о случившемся немедленно сообщается непосредственному руководителю и в ОКЗИ.

4. Контроль за организацией и обеспечением защиты информации

4.1. Государственный контроль за организацией и обеспечением защиты информации при ее передаче по каналам связи с использованием СКЗИ осуществляют органы Федеральной службы безопасности Российской Федерации.

4.2. ОКЗИ контролирует организацию и обеспечение защиты информации, с использованием СКЗИ, а также выполнение пользователями условий использования СКЗИ, установленных эксплуатационной и технической документацией к ним и Инструкцией ФАПСИ № 152 от 13 июня 2001 г. «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».

4.3. Специалист, ответственный за эксплуатацию СКЗИ контролирует выполнение пользователями условий использования СКЗИ, установленных эксплуатационной и технической документацией к ним и Инструкцией ФАПСИ № 152 от 13 июня 2001 г. «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» в рамах организации, руководствуясь Инструкцией ответственного за эксплуатацию СКЗИ (Приложение № 3).

4.4. При обнаружении недостатков в использовании СКЗИ пользователи обязаны принять безотлагательные меры к их устранению. Сообщения о принятых мерах должны быть представлены в установленные проверяющими сроки.

4.5. Если в использовании СКЗИ выявлены серьезные нарушения, из-за чего становится реальной утечка информации, безопасность которой обеспечивается с использованием СКЗИ, то органы государственного контроля и ОКЗИ вправе дать указание о немедленном прекращении использования СКЗИ до устранения причин выявленных нарушений.

5. Нормативные документы, которые проверяют контролирующие органы

№ п/п	Проверяемые контролирующим органом требования		Перечень представляемых документов и справок	Нормативные правовые акты, требования которых подлежат проверке, в соответствии с которыми также ведется разработка организационно-правовой документации
1	Организационные меры защиты персональных данных	область применения СКЗИ в информационных системах персональных данных	Приказ о назначении ответственного за эксплуатацию СКЗИ **(Приложение № 2)** Должностная инструкция ответственного за эксплуатацию СКЗИ **(Приложение № 3)**	Приказ Федеральной службы безопасности России от 10 июля 2014 г. № 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».
		наличие ведомственных документов и приказов по организации криптографической защиты информации		
		выполнение рекомендаций и указаний ФСБ России (при их наличии) по вопросам организации связи с использованием криптосредств		
2	Организация системы криптографических мер защиты информации	наличие модели угроз нарушителя	Модель угроз, разработанная оператором (на каждую информационную систему). Документы по поставке СКЗИ оператору (государствен-	Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных, эксплуатируемых при осуществлении соответствующих
		соответствие модели угроз исходным данным		
		соответствие требуемого уровня криптографической защиты полученной модели нарушителя		
		соответствие используемых СКЗИ полученному уровню криптографической защиты		
		наличие документов по поставке СКЗИ оператору		

			ный контракт)	видов деятельности № 149/7/2/6/-432 от 31.03.2015 г.
3	Разрешительная и эксплуатационная документация	наличие необходимых лицензии для использования СКЗИ в информационных системах персональных данных	Лицензии и сертификаты на используемые СКЗИ. Эксплуатационная документация на СКЗИ.	Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)
		наличие сертификатов соответствия на используемые СКЗИ		
		наличие эксплуатационной документации на СКЗИ (формуляров, правил работы, руководств оператора и т.п.)		
		порядок учета СКЗИ, эксплуатационной и технической документации к ним		
		выявление не сертифицированных ФСБ России СКЗИ (запрещено использование не сертифицированных СКЗИ)		
4	Требования к обслуживающему персоналу	порядок учета лиц, допущенных к работе с СКЗИ предназначенными для обеспечения безопасности персональных данных в информационной системе	Приказ о назначении лиц, допускаемых к самостоятельной работе с СКЗИ **(Приложение № 4)** Заключение о допуске к самостоятельной работе с СКЗИ **(Приложение № 5)** Документы, подтверждающие функциональные обязанности сотрудников (инструкция пользователя СКЗИ) **(Приложение № 6)**	Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положе-
		наличие функциональных обязанностей пользователей СКЗИ		
		укомплектованность штатных должностей личным составом, а также достаточность имеющегося личного состава для решения задач по организации криптографической защиты информации		
		организация процесса обучения лиц, использующих СКЗИ применяемых в информационных системах, правилам работы с ними и другим нормативным документам по организации работ (связи) с использование СКЗИ		

			Документы, подтверждающие прохождение обучения сотрудников по вопросам ЗИ (Журнал учета обучения пользователей средств криптографической защиты информации) **(Приложение № 7)**	ние ПКЗ-2005)
5	Оценка соответствия применяемых СКЗИ	-соответствие программного обеспечения, реализующего криптографические алгоритмы используемых СКЗИ эталонным версиям, прошедших сертификацию в ФСБ России проведение (при необходимости) на местах осуществления проверки оперативных тематических исследований, используемых СКЗИ	Средства СКЗИ. Программное обеспечение СКЗИ (дистрибутив).	Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)
6	Эксплуатация СКЗИ	проверка правильности ввода СКЗИ в эксплуатацию и соответствие условий эксплуатации технических средств удостоверяющего центра (при наличии) требованиям эксплуатационной документации и сертификатов соответствия оценка технического состояния СКЗИ, соблюдения сроков и полноты проведения технического обслуживания, а также проверка соблюдения правил пользования СКЗИ и порядка обращения с ключевыми документами к ним	Акты ввода СКЗИ в эксплуатацию **(Приложение № 8)** Журнал поэкземплярного учета СКЗИ **(Приложение № 9)** Журнал учета и выдачи носителей с ключевой информацией **(Приложение № 10)**	Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утвержде-

			Книга лицевых счетов пользователей СКЗИ, эксплуатационной и технической документации к ним, ключевых документов **(Приложение № 11)**	нии Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)
7	Организационные меры	выполнение требований по размещению, специальному оборудованию, охране и организации режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним, а также соответствие режима хранения СКЗИ и ключевой документации предъявляемым требованиям	Эксплуатационная документация на СКЗИ Помещения, выделенные для установки СКЗИ и хранения ключевых документов к ним Инструкция по восстановлению связи в случае компрометации действующих ключей к СКЗИ **(Приложение № 12)**	Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)
		оценка степени обеспечения оператора криптоключами и организации их доставки		
		проверка наличия инструкции по восстановлению связи в случае компрометации действующих ключей к СКЗИ		
		порядок проведения разбирательств и составления заключений по фактам нарушения условий хранения носителей персональных данных или использования СКЗИ		

Приложение № 1
к Методическим рекомендациям

Основные законодательные акты в сфере обеспечения защиты информации средствами криптографической защиты информации

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

– Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством российской федерации требований к защите персональных данных для каждого из уровней защищенности»;

– Инструкция ФАПСИ № 152 от 13 июня 2001 г. «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»;

– Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности № 149/7/2/6/-432 от 31.03.2015 г.

Приложение № 2
к Методическим рекомендациям

Приказ о назначении ответственного за эксплуатацию СКЗИ

ПРИКАЗ

от «___» _____ 20____ № _____

О назначении ответственного
за эксплуатацию СКЗИ

В целях организации и обеспечения эксплуатации СКЗИ в
_____
(наименование организации)

п р и к а з ы в а ю:

1. Назначить Ответственным лицом за эксплуатацию СКЗИ _____. Во время отсутствия обязанности Ответственного за эксплуатацию СКЗИ возлагать на _____.
2. Ответственному за эксплуатацию СКЗИ при организации и обеспечении работы с СКЗИ и криптографическими ключами руководствоваться Инструкцией ответственного за эксплуатацию СКЗИ _____
(наименование организации)
3. Контроль за исполнением настоящего приказа возложить на _____.

Руководитель организации _____ _____

Приложение № 3
к Методическим рекомендациям

Инструкция ответственного за эксплуатацию СКЗИ

1. Общие положения

1.1 Все действия с СКЗИ осуществляются в соответствии с эксплуатационной документацией на СКЗИ.

1.2 Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами приказом назначается ответственный за эксплуатацию СКЗИ.

Ответственный за эксплуатацию СКЗИ осуществляет:

- поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним;
- учет пользователей СКЗИ;
- обучение пользователей правилам эксплуатации СКЗИ;
- контроль за соблюдением условий использования СКЗИ в соответствии с эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;
- расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;
- разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

1.3 Текущий контроль, обеспечение функционирования и безопасности СКЗИ возлагается на ответственного за эксплуатацию СКЗИ.

1.4 Ответственный за эксплуатацию СКЗИ должен быть ознакомлен с настоящей Инструкцией под расписку.

2. Учет и хранение СКЗИ и криптографических ключей

2.1 СКЗИ, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.

2.2 Поэкземплярный учет СКЗИ ведет ответственный за эксплуатацию СКЗИ в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним (далее – Журнал). При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

2.3 Все полученные экземпляры СКЗИ, криптографических ключей должны быть выданы под расписку в Журнале пользователям СКЗИ, несущим персональную ответственность за их сохранность.

2.4 Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к СКЗИ, инструкции хранятся у ответственного за эксплуатацию СКЗИ. Криптографические ключи хранятся у пользователей СКЗИ. Хранение осуществляется в закрываемых на замок металлических хранилищах пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение, или в опечатанном пенале (тубусе). Металлические шкафы должны быть оборудованы внутренними замками с двумя экземплярами ключей, кодовыми замками и приспособлениями для опечатывания. Один экземпляр ключа от хранилища должен находиться у ответственного за эксплуатацию СКЗИ, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в специальном сейфе.

2.5 На ключевые носители с изготовленными криптографическими ключами наклеиваются наклейки, содержащие надписи: на один ключевой носитель - «Рабочий»; на другой ключевой носитель - «Резервный».

2.6 Ключевой носитель с наклейкой «Резервный» помещается в конверт и опечатывается пользователем и ответственным за эксплуатацию СКЗИ.

2.7 Все полученные экземпляры криптографических ключей должны быть выданы под расписку в Журнале. Резервные криптографические ключи могут находиться на хранении у ответственного за эксплуатацию СКЗИ.

2.8 Ключевые носители с неработоспособными криптографическими ключами ответственный за эксплуатацию СКЗИ принимает от пользователя под расписку в Журнале. Неработоспособные ключевые носители подлежат уничтожению.

2.9 При необходимости замены наклейки на ключевом носителе (стирание надписи реквизитов) пользователь передает его ответственному за эксплуатацию СКЗИ, который в присутствии пользователя снимает старую наклейку и приклеивает новую наклейку с такими же учетными реквизитами.

2.10 Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

2.11 СКЗИ и криптографические ключи могут доставляться специальной (фельдъегерской) связью или курьером, имеющего доверенность, подписанную руководителем, на право получения СКЗИ, при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ и криптографическим ключам во время доставки.

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

2.13 Для пересылки СКЗИ, эксплуатационной и технической документации к ним, криптографических ключей составляется Акт приема-передачи (Опись) документов, в котором указывается: что посылается и в каком количестве, учетные

номера СКЗИ, криптографических ключей или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Акт приема-передачи (Опись) документов вкладывается в упаковку.

2.14 Полученную упаковку вскрывает только лицо, для которого она предназначена. Если содержимое полученной упаковки не соответствует указанному в Акте приема-передачи (Описи) документов или сама упаковка и оттиск печати - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то должен быть составлен акт о происшедшем нарушении. Полученные с такими отправлениями СКЗИ и криптографические ключи до получения указаний от руководителя применять не разрешается.

2.15 При обнаружении бракованных криптографических ключей ключевой носитель с такими ключами следует возвратить для установления причин происшедшего и их устранения в дальнейшем. В этом случае необходимо получить новые криптографические ключи.

2.16 Ключевые носители совместно с Журналом должны храниться ответственным за эксплуатацию СКЗИ в сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и Журнал совместно с другими документами, при этом ключевые носители и Журнал должны быть помещены в отдельную папку.

2.17 На время отсутствия ответственного за эксплуатацию СКЗИ должен быть назначен сотрудник его замещающий.

2.18 При необходимости криптографические ключи сдаются на временное хранение ответственному за эксплуатацию СКЗИ.

4. Использование СКЗИ и криптографических ключей

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

4.2. Криптографический ключ невозможно использовать, если истек срок действия.

4.3. Для обеспечения контроля доступа к СКЗИ системный блок ПЭВМ опечатывается ответственным за эксплуатацию СКЗИ.

4.4. Пользователь должен периодически (ежедневно) проверять сохранность оборудования и целостность печатей на ПЭВМ. В случае обнаружения «посторонних» (не зарегистрированных) программ или выявления факта повреждения печати на системном блоке ПЭВМ работа должна быть прекращена**.** По данному факту проводится служебное расследование, и осуществляются работы по анализу и ликвидации последствий данного нарушения.

4.5. При выявлении сбоев или отказов пользователь обязан сообщить о факте их возникновения ответственному за эксплуатацию СКЗИ и предоставить ему носители криптографических ключей для проверки их работоспособности. Проверку работоспособности носителей криптографических ключей ответственный за эксплуатацию СКЗИ выполняет в присутствии пользователя.

4.6. В случае, если рабочие криптографические ключи потеряли работоспо-

собность, то по просьбе пользователя ответственный за эксплуатацию СКЗИ, вскрывает конверт (коробку) с резервными криптографическими ключами, делает копию ключевого носителя, используя резервные криптографические ключи, помещает резервные криптографические ключи в конверт (коробку), а на новый ключевой носитель наклеивает наклейку с надписью «Рабочий».

4.7. В экстренных случаях, не терпящих отлагательства, вскрытие конверта (коробки) с резервными криптографическими ключами может осуществляться комиссионно с последующим уведомлением ответственного за эксплуатацию СКЗИ о факте вскрытия конверта с криптографическими ключами. На конверте делается запись о вскрытии с указанием даты и времени вскрытия конверта и подписью пользователя. Вскрытый конверт вместе с неработоспособными криптографическими ключами сдаются ответственному за эксплуатацию СКЗИ.

4.8. Вскрытие системного блока ПЭВМ, на которой установлено СКЗИ, для проведения ремонта или технического обслуживания должно осуществляться в присутствии ответственного за эксплуатацию СКЗИ.

5. Изготовление и плановая смена криптографических ключей

5.1. Изготовление криптографических ключей может производиться администратором безопасности в присутствии пользователя.

5.2. Криптографические ключи изготавливаются на отчуждаемый ключевой носитель (электронный идентификатор) в соответствии с эксплуатационно-технической документацией на СКЗИ и требованиями безопасности, установленными настоящей Инструкцией.

5.3. В целях обеспечения непрерывности проведения работы, плановую смену криптографических ключей следует производить заблаговременно, до окончания срока действия закрытых криптографических ключей.

5.4. При замене криптографических ключей используют программное обеспечение в соответствии с документацией по эксплуатации.

Приложение № 4
к Методическим рекомендациям

Приказ о назначении лиц, допускаемых к самостоятельной работе с СКЗИ

ПРИКАЗ

«___» _____ 201_ г. № _____

О назначении лиц, допускаемых
к самостоятельной работе с СКЗИ

Для осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

п р и к а з ы в а ю:

1. К работе с СКЗИ допустить следующих пользователей:

№ п/п	ФИО пользователя	Структурное подразделение	Должность

2. Контроль за исполнением настоящего приказа возложить на _____.

Руководитель организации _____

Приложение № 5
к Методическим рекомендациям

Утверждаю
Руководитель подразделения

Заключение о допуске к самостоятельной работе с СКЗИ

Структурное подразделение _____
Должность_____
Фамилия, имя, отчество_____
с "_____"_____ 20__ г. по "_____"_____ 20__ г. в соответствии с Программой обучения, утвержденной смоленским областным государственным автономным учреждением «Центр информационных технологий» от "_____"_____20__ г. прошел(ла) подготовку по правилам работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну и сдал(а) зачет с общей оценкой_____.

По решению комиссии _____ допущен(а) к самостоятельной работе со средствами криптографической защиты информации.

Председатель комиссии:

_____

Члены комиссии:

_____

_____

_____

«___» _____ 20___ г.

Приложение № 6
к Методическим рекомендациям

ИНСТРУКЦИЯ
пользователя средств криптографической защиты информации

Пользователи СКЗИ обязаны:

- не разглашать конфиденциальную информацию, к которой они допущены, и сведения о криптоключах;
- соблюдать требования по обеспечению безопасности информации с использованием СКЗИ;
- сообщать специалисту ответственному за эксплуатацию СКЗИ о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах;
- сдать специалисту ответственному за эксплуатацию СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- немедленно уведомлять специалиста ответственного за эксплуатацию СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов, ключей от помещений, сейфов, личных печатей.

Пользователи СКЗИ несут персональную ответственность за сохранность СКЗИ и ключевых документов.

Не допускается:

- производить несанкционированное копирование ключевых документов;
- знакомить или передавать ключевые документы лицам, к ним не допущенным;
- выводить ключевые документы на дисплей или принтер;
- вставлять носители ключевой информации в считывающие устройства других компьютеров;
- оставлять носители ключевой информации без присмотра на рабочем месте;
- записывать на носители ключевой информации посторонние файлы.

Приложение № 7
к Методическим рекомендациям

ЖУРНАЛ
учета обучения пользователей
средств криптографической защиты информации

№ п/п	Должность	Ф.И.О. Пользователя СКЗИ	Номер и дата Приказа о назначении	Программа обучения	Дата проведения обучения	Подпись обучаемого, дата	Подпись лица, проводившего обучение, дата
1	2	3	4	5	6	7	8

Приложение № 8
к Методическим рекомендациям

УТВЕРЖДАЮ
Руководитель _____
(Организации-заявителя)
_____ А.А. Иванов
"__" _____ 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))
(ответственный за эксплуатацию СКЗИ) 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) _____
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 ЖТЯИ. _____ выведен на бумажный носитель, раздел 11 Формуляра заполнен установленным порядком, Формуляр передан на ответственное хранение пользователю АРМ Заявителя.

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;
- сдать установочный комплект СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- 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.

Акт составлен в двух экземплярах.

_____/_____/_____
(должность ответственного за эксплуатацию СКЗИ) (подпись) (Фамилия И.О.)

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

Приложение № 9
к Методическим рекомендациям

ТИПОВАЯ ФОРМА
ЖУРНАЛА ПОЭКЗЕМПЛЯРНОГО УЧЕТА СКЗИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ
(ДЛЯ ОБЛАДАТЕЛЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним,ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		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	10	11	12	13	14	15	16

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 Петрова П.П., 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 № 10
к Методическим рекомендациям

Журнал
поэкземплярного учета ключевых документов

№ п/п	Наименование ключевых документов	Дата изготовления ключевых документов	Ф.И.О. сотрудника, изготовившего ключевые документы	Тип МНИ	Номера экземпляров ключевых документов	Отметка о выдаче		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении	
						Кому выданы (фамилия инициалы)	Расписка в получении и дата			Ф.И.О. лица, лица проводившего уничтожение	Дата, расписка об уничтожении
1	2	3	4	5	6	7	8	9	10	11	12
Пример заполнения											
1	*Ключ ЭП Петрова П.П.*	*20.08.2011*	*Иванов И.И.*	*Дискета*	*Экз. № 1, 2*	*Петров П.П.*		*25.08.2011*	*25.08.2011*	*Петров П.П.*	
2	*Ключ аутентификации*	*20.08.2011*	*Иванов И.И.*	*Дискета*	*Экз. № 1,2*	*Петров П.П.*		*25.08.2011*	*25.08.2011*	*Иванов И.И.*	

Примечание:
1. Журнал ведется специалистом ответственным за эксплуатацию СКЗИ.
2. Тип съемных машинных носителей информации (МНИ), применяемых для хранения ключевой информации, определяется Участником СЭДФК.
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 Петрова П.П., 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 № 11
к Методическим рекомендациям

**Книга лицевых счетов пользователей СКЗИ,
эксплуатационной и технической документации к ним, ключевых документов**

Начата « » 201 г.

Должность

ФИО должностного лица

Окончена « » 201 г.

Должность

ФИО должностного лица

Опись лицевых счетов

№ п/п	ФИО	№ по картотеке	Расписка лица, оформившего л/с

ЛИЦЕВОЙ СЧЕТ №

Пользователь СКЗИ:

_____

(должность)

_____

(ФИО)

Наименование СКЗИ	Серийные номера СКЗИ	Регистрационные номера экземпляров ключевых документов	Дата и номер подтверждения или расписка о получении СКЗИ	Дата и номер подтверждения или расписка о возвращении / уничтожении СКЗИ	Примечания

Приложение № 12
к Методическим рекомендациям

УТВЕРЖДАЮ

Руководитель

[Название организации]

_____ _____

«_____» _____ 201_ г.

ИНСТРУКЦИЯ

по восстановлению связи в случае компрометации действующих ключей к СКЗИ [Название организации]

1. Под компрометацией индивидуального ключа понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность конфиденциальной информации. К событиям, связанным с компрометацией действующих криптографических ключей, относится:

- утрата (в том числе хищение) ключевых дискет (флэш - накопителей) с последующим их обнаружением;
- увольнение пользователей, имевших доступ к ключевой информации;
- передача ключевой информации по линии связи в открытом виде (если это не предусмотрено правилами пользования);
- нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;
- возникновение подозрений на утечку информации или ее искажение;
- не расшифровывание входящих или исходящих сообщений;
- отрицательный результат при проверке электронной цифровой подписи документа;
- нарушение целостности упаковки ключевых дискет (флэш - накопителей) и (или) печати на сейфе, где хранились ключевые дискеты (флэш - накопители);
- несанкционированное копирование ключевых дискет (флэш - накопителей);
- случаи, когда нельзя достоверно установить, что произошло с магнитными носителями, содержащими ключевую информацию (в том числе, случаи, когда магнитный носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате злоумышленных действий).

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

2. При наступлении любого из перечисленных выше событий пользователь должен немедленно прекратить связь с другими пользователями и сообщить о факте компрометации (или предполагаемом факте компрометации) ответственному за эксплуатацию СКЗИ.

3. Расследование факта компрометации (или предполагаемой компрометации) должно проводиться на месте происшествия специально назначаемой комиссией во главе с ответственным за эксплуатацию СКЗИ.

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.

4. Для восстановления конфиденциальной связи после компрометации ключей пользователь обращается к ответственному за эксплуатацию СКЗИ с целью регистрации вновь изготовленных (или резервных) ключей. Регистрация новых ключей шифрования и ЭП осуществляется тем же порядком, как и при плановой смене ключей.

С инструкцией ознакомлены пользователи СКЗИ:

_____/_____/

_____/_____/

_____/_____/

_____/_____/

_____/_____/

_____/_____/

_____/_____/

_____/_____/

_____/_____/

Приложение № 13
к Методическим рекомендациям

Программа подготовки (обучения) пользователей правилам работы с средствами криптографической защиты информации

1. ВВЕДЕНИЕ

Программа подготовки (обучения) разработана в соответствии с законодательными, нормативными и методическими документами в области информационной безопасности и рекомендациями ФСБ России.

Программа обучения учитывает требования:

- Федерального закона от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;

- Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- постановления Правительства Российской Федерации от 16 апреля 2012 г. № 313 «О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

- приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

- положения «О разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденных Приказом ФСБ России от 9 февраля 2005 г. № 66;

- инструкции о порядке работы с криптографическими средствами;

- технической и эксплуатационной документации на средства криптографической защиты информации (далее – СКЗИ).

Цель подготовки (обучения) по программе

Целью подготовки (обучения) является введение пользователей в предметную область информационной безопасности и ознакомление с правилами работы с СКЗИ.

Аудитория

Сотрудники органов исполнительной власти Смоленской области, их подведомственные учреждения и органы местного самоуправления муниципальных образований Смоленской области, использующие в своей работе СКЗИ для обработки и передачи по каналам связи информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Краткий обзор

Учебная программа состоит из основных разделов:

- общие вопросы защиты информации;
- организация обеспечения защиты конфиденциальной информации при использовании электронной подписи в документообороте органов исполнительной власти Смоленской области;
- правила работы с СКЗИ.

2. ПЕРЕЧЕНЬ ТЕМ

№ п/п	Тема
I.	**Основы безопасности информационных технологий**
1.1	Основные понятия информационной безопасности
1.2	Угрозы безопасности информационных технологий
1.3	Виды мер и основные принципы обеспечения информационной безопасности
II	**Обеспечение безопасности конфиденциальных данных**
2.1.	Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»
2.2.	Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»
2.3	Положение «О разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное Приказом ФСБ России от 9 февраля 2005 г. № 66;
III	**Правила работы с СКЗИ**
3.1.	Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»
3.2.	Порядок использования СКЗИ КриптоПро CSP и ViPNet CSP
3.3.	Порядок использования электронной подписи
3.4.	Информационная система «ДелоPro». Делопроизводство и документооборот.
IV	**Тест для зачета**

3. РЕФЕРАТИВНОЕ ОПИСАНИЕ ТЕМ

Модуль 1. Основы безопасности информационных технологий

1.1 Основные понятия информационной безопасности

Что такое безопасность информационных технологий. Субъекты информационных отношений, их интересы и безопасность, пути нанесения им ущерба. Основные термины и определения. Конфиденциальность, целостность, доступность. Определение НСД. Объекты, цели и задачи защиты информационных систем и циркулирующей в них информации.

1.2 Угрозы безопасности информационных технологий

Угрозы безопасности информации, информационных систем и субъектов информационных отношений. Основные источники и пути реализации угроз. Классификация угроз безопасности и каналов проникновения в автоматизированную систему и утечки информации. Основные непреднамеренные и преднамеренные искусственные угрозы. Классификация нарушителей информационной безопасности.

1.3 Виды мер и основные принципы обеспечения информационной безопасности

Виды мер противодействия угрозам безопасности (организационные, технические, физические). Достоинства и недостатки различных видов мер защиты. Основные принципы построения системы обеспечения безопасности информации в информационной системе.

Модуль 2. Обеспечение безопасности конфиденциальных данных

2.1. Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»

Основные положения. Требования, предъявляемые к оператору конфиденциальной информации. Положение о лицензировании деятельности по технической защите конфиденциальной информации.

2.2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Сфера действия. Основные понятия. Информация как объект правовых отношений. Обладатель информации. Право на доступ к информации. Защита информации.

2.3. Положение «О разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное Приказом ФСБ России от 9 февраля 2005 г. N 66

Общие положения. Порядок разработки СКЗИ. Порядок производства СКЗИ. Порядок реализации (распространения) СКЗИ. Порядок эксплуатации СКЗИ.

Модуль 3. Правила работы с СКЗИ

3.1. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

Основные положения. Риски использования ЭП. Порядок обращения с ключевыми носителями. Инфраструктура открытых ключей. Управление своими сертификатами, их отзыв, приостановка и возобновление действия. Действия при истечении сертификата, компрометации ключей и прочих нестандартных ситуациях. Резервное копирование ключей, условия хранения и управления своими ключевыми данными.

3.2. Порядок использования СКЗИ КриптоПро CSP и ViPNet CSP

Установка и настройка СКЗИ. Хранение, использование, учет и контроль за использованием СКЗИ. Проверка срока действия сертификата ЭП.

3.3. Порядок использования электронной подписи

Основные понятия. Сфера регулирования отношений в области использования электронных подписей. Принципы использования электронной подписи. Виды электронной подписи. Признание квалифицированной электронной подписи. Средства электронной подписи. Удостоверяющий центр. Сертификат ключа проверки электронной подписи. Аккредитация удостоверяющего центра.

Модуль 4. Тест для зачета

Анкета для опроса пользователей СКЗИ

Заполняется персонально пользователем СКЗИ

ФИО _____

Для корректного заполнения просьба отметить один или несколько вариантов ответа

1. Какие свойства информации необходимо защищать?
    a) коммерческую тайну;
    b) целостность;
    c) конфиденциальность;
    d) полноту информации;
    e) доступность.

2. Кто может быть нарушителем безопасности?
    a) посетители;
    b) сотрудники Вашей организации, не прошедшие обучение по работе с СКЗИ;
    c) сотрудники Вашей организации, прошедшие обучение по работе с СКЗИ;
    d) все вышеперечисленные.

3. Вопрос 3…..

4. Вопрос 4…..

5. Вопрос 5…..

6. Вопрос 6…..

7. Вопрос 7…..

8. Вопрос 8…..

9. Вопрос 9…..

10. Вопрос 10…..

11. Вопрос 11…..

12.Вопрос 12…..

13.Вопрос 13…..

14.Вопрос 14…..

15. Осуществляется ли обработка конфиденциальной информации в присутствии посторонних лиц?
    a) да, если монитор расположен таким образом, что исключается возможность его обзора;
    b) нет, ни в коем случае;
    c) да, если это сотрудник лицензиата Управления Федеральной службы безопасности по Смоленской области.

Подпись _____

Дата _____

Результаты проверки

Всего ответов _____(кол-во)

Правильных ответов _____(кол-во)

(зачтено/не зачтено)

Проверил

ФИО, подпись_____