|  |
| --- |
|   |
|  **АДМИНИСТРАЦИЯ УСВЯТСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ** **ДОРОГОБУЖСКОГО РАЙОНА СМОЛЕНСКОЙ ОБЛАСТИ** **Р А С П О Р Я Ж Е Н И Е**  |
| от 06.08.2019 года № 88 -рОб утверждении документов по обеспечению безопасности конфиденциальной информации с использованием средств криптографической защиты в Администрации Усвятского сельского поселения Дорогобужского района Смоленской области 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», в целях обеспечения защиты информации и режима безопасности персональных данных работников учреждения и лиц, обращающихся за получением муниципальных услуг в Администрацию Усвятского сельского поселения Дорогобужского района Смоленской области 1. Утвердить Положение об организации и проведении работ по обеспечению безопасности конфиденциальной информации с использованием средств криптографической защиты в Администрации Усвятского сельского поселения Дорогобужского района Смоленской области, далее – Положение (Приложение № 1). 2. Утвердить программу обучения работников Администрации Усвятского сельского поселения Дорогобужского района Смоленской области по правилам работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну (Приложение №2).3. Утвердить Инструкциюответственного пользователя СКЗИ в Администрации Усвятского сельского поселения Дорогобужского района Смоленской области (Приложение №3).4. Утвердить инструкцию о порядке действий при компрометациикриптоключей (Приложение №4).5. Утвердить состав комиссии по допуску пользователей СКЗИ к самостоятельной работе с СКЗИ (Приложение №5).6. Контроль за исполнением настоящего распоряжения оставляю за собой. |

Глава муниципального образования

Усвятское сельское поселение

Дорогобужского района Смоленской области **Л.П. Павликов**

Приложение №1

к распоряжению Администрации

Усвятского сельского поселения

Дорогобужского района

Смоленской области

от 06.08.2019 г. № 88-р

**Положение**

 **об организации и проведении работ по обеспечению безопасности конфиденциальной информации с использованием средств криптографической защиты в Администрации Усвятского сельского поселения Дорогобужского района Смоленской области**

**1. Общие положения**

1.1. Настоящий порядок разработан для практического применения пользователями средств криптографической защиты информации (далее - СКЗИ) в Администрации Усвятского сельского поселения Дорогобужского района Смоленской области «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 Администрации Усвятского сельского поселения Дорогобужского района Смоленской области (далее – Администрация) определяются должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СКЗИ.

1.3. В Администрации 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, при необходимости, 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 Администрацию в соответствии с распоряжением Главы муниципального образования Усвятское сельское поселение Дорогобужского района Смоленской области 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 Администрации на основании принятого зачета по программе подготовки (обучения).

6.3. Программа подготовки к самостоятельной работе с СКЗИ 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 Администрации 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 Администрации в качестве преподавателей.

6.5. Пользователи, допущенные к работе с СКЗИ регистрируются в журнале учета обучения Пользователей СКЗИ (Приложение 4).

Приложение № 1

к Положению об организации и проведении работ

по обеспечению безопасности конфиденциальной информации

с использованием средств криптографической защиты

**Журнал**

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

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Регистрационный номер | Наименованиехранилища(сейф,металлическийшкаф, кладовая,спецхранилище) | Заводской,инвентарныйномерхранилища | Местонахождение хранилища(подразделение, номеркомнаты,корпуса,здания) | Чтохранится(документы,изделия) | Фамилияответственного захранилище | КоличествоКомплектовключей и ихномера | РаспискаОтветственногоза хранилище вполученииключа и дата | Расписка вобратномприемеключа 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

**Журнал**

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №п/п | Наименование СКЗИ,Эксплуатационной итехническойдокументации к ним,ключевыхдокументов | СерийныеномераСКЗИ,ЭксплуАтационной итехническойдокументациик ним,номера серийключевыхдокументов | Номераэкземпляров(криптографическиеномера)ключевыхдокументов | Отметка о получении | Отметка о подключении(установке) СКЗИ | Отметка о подключении(установке) СКЗИ | Отметка об изъятии СКЗИ из аппаратныхсредств, уничтожении ключевыхдокументов | Примечание |
| От когополучены | Дата иномерсопроводительного письма | Ф.И.О.пользователя СКЗИ | Дата ираспискавполучении | Ф.И.О.сотрудниковорганакриптографическойзащиты,пользователяСКЗИ,Произведшихподклюючение(установку) | Датаподключения(установки) иподписилиц,произведшихподклюючение (установку) | НомераАппаратныхсредств,в которыеустановлены или ккоторымподключены СКЗИ | Датаизъятия(уничтожения) | Ф.И.О.Сотруниковорганакриптографическойзащиты,пользователяСКЗИ,ПроизВодившихизъятие(уничтожение) | Номеракта илираспискаобуничтожении |
| 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

**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 распоряжением Главы муниципального образования Усвятское сельское поселение Дорогобужского района Смоленской области

" \_\_\_\_\_ " \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 \_\_ г. № \_\_\_\_\_\_,

прошел(ла)подготовку поправилам 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

**Журнал**

**учета обучения пользователей средств криптографической защиты информации**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| №п/п | Должность | Ф.И.О.пользователяСКЗИ | Номер и датаприказа оназначении | Программаобучения | Период проведения обучения | Подписьобучаемого поитогамобучения,дата | Подпись лица,проводившегообучение, дата |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  |  |  |  |  |  |  |  |

Приложение №2

к распоряжению Администрации

Усвятского сельского поселения

Дорогобужского района

Смоленской области

от 06.08.2019 г. № 88-р

**ПРОГРАММА**

**обучения работников Администрации Усвятского сельского поселения Дорогобужского района Смоленской области по правилам работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну**

**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 Администрации Усвятского сельского поселения Дорогобужского района 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 криптографиче-ской 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. Имеет ли юридическую силу электронная подпись, если она используется не в соответствии со сведениями, указанными в сертификате ключа электронной подписи?

a) нет

b) не всегда

c) да

4. Подлежат ли поэкземплярному учету (в журнале учета)
используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы?

a) да

b) нет

5. На время отсутствия пользователей СКЗИ должны:

a) удаляться

b) быть не активны( выключен монитор)

c) При наличии технической возможности быть выключены, отключены от линии связи и убраны в опечатываемые хранилища

6. Что необходимо сделать с выведенными из действия криптоключами?

a) разгласить

b) уничтожить

c) скопировать

7. Является ли увольнение сотрудника, имеющего доступ к
ключевым носителям или к ключевой информации на данных носителях,
поводом для замены электронной подписи?

a) да

b) нет

8.Кем осуществляется контроль за соблюдением правил
пользования СКЗИ и условий их использования?

a) Обладателем и пользователем(потребителем) защищаемой информации

b) ФСБ России

c) ФСБ России, обладателем и пользователем (потребителем) защищаемой информации

9. Владелец сертификата ключа подписи обязан:

a) Хранить в тайне закрытый ключ электронной подписи

b) Хранить в тайне открытый и закрытый ключ электронной подписи

c) Хранить в тайне открытый ключ электронной подписи

10. Удостоверяющий центр, выдавший сертификат ключа проверки
электронной подписи, обязан аннулировать его:

a) по заявлению в письменной форме любого пользователя информационной системы

b) удостоверяющий центр не имеет права аннулировать сертификаты ЭП

c) по заявлению в письменной форме владельца сертификата ключа проверки электронной подписи

11. В соответствии с приказом ФАПСИ №152 от 13 июня 2001 г.
непосредственно к работе с СКЗИ пользователи допускаются только после
соответствующего обучения. Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе  с СКЗИ, является:

a) Акт о готовности к эксплуатации СКЗИ

b) Заключение о допуске ответственного лица к самостоятельной работе с СКЗИ

c) Заявление на ЭП

12. Что подтверждает юридическую значимость электронной подписи в документе?

a) Сертификат ключа проверки электронной подписи

b) Открытый ключ проверки электронной подписи

c) Договор оказания услуг

13. Что входит в обязанности пользователей СКЗИ?

a) Все ответы верны

b) Сообщать в ОКЗ о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним

c) Соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа

d) Сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями

14. Какие действия необходимо провести с Криптоключами, в отношении которых возникло подозрение в компрометации?

a) Сообщить в соответствующий орган криптографической защиты

b) Необходимо немедленно вывести из действия

c) сообщить о факте компрометации (или предполагаемом факте компрометации) ответственному за эксплуатацию СКЗИ

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\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**План**

**обучения работников Администрации Усвятского сельского поселения Дорогобужского района Смоленской области правилам работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №п/п | Изучаемые вопросы | Количество часов | Форма (метод) подготовки | Лицо, ответственное за проведение мероприятия |
| 1 | 2 | 3 | 4 | 5 |
| 1 | Организация защитыИнформации 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 офиснымиприложениями; работа с базами данных. Порядокприменения СКЗИ. | 4 | Практическоезанятие | Администраторбезопасности |
| 7 | Порядокпредставленияконфиденциальныхданных в электронномвиде потелекоммуникационнымканалам связи с помощью АИС МФЦ и ПК ПВД в рамках организации предоставления муниципальныхуслуг | 2 | Практическоезанятие | Администраторбезопасности |

Приложение №3

к распоряжению Администрации

Усвятского сельского поселения

Дорогобужского района

Смоленской области

от 06.08.2019 г. № 88-р

**Инструкция**

**ответственного пользователя СКЗИ в Администрации Усвятского сельского поселения Дорогобужского района Смоленской области**

**1. Общие положения**

1.1. Настоящая Инструкция ответственного пользователя средств криптографической защиты информации в Администрации Усвятского сельского поселения Дорогобужского района Смоленской области (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 Администрации Усвятского сельского поселения Дорогобужского района Смоленской области (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

Администрации Усвятского сельского поселения Дорогобужского района Смоленской области (далее – Администрация), 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 распоряжением Главы муниципального образования Усвятское сельское поселение Дорогобужского района Смоленской области.

1.5. На время отсутствия Ответственного пользователя криптосредств его обязанности исполняет другой специалист, с которым предварительно проводится инструктаж по обслуживанию криптосредств в Администрации. 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 системе Администрации 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 Главе муниципального образования Усвятское сельское поселение Дорогобужского района смоленской области.

2.21. Немедленно уведомлять ответственного за обеспечение безопасности персональных данных в информационной системе Администрации 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 системе Администрации.

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 Главы муниципального образования Усвятское сельское поселение Дорогобужского района Смоленской области 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 Администрации 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 Администрации

Усвятского сельского поселения

Дорогобужского района Смоленской области

**Журнал**

**учета пользователей криптосредств в Администрации Усвятского сельского поселения Дорогобужского района Смоленской области**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№****п/п** | **Ф.И.О. пользователя** | **Серийный номер****лицензии** | **Номер****дистрибутива** | **Примечание** |
| **1** | **2** | **3** | **4** | **5** |
| 1. |  |  |  |  |
| 2. |  |  |  |  |

Приложение№2

к Инструкции ответственного пользователя средств

криптографической защиты информации

в информационной системе в Администрации

Усвятского сельского поселения

Дорогобужского района Смоленской области

УТВЕРЖДАЮ

Глава муниципального образования

Усвятское сельское поселение

Дорогобужского района

Смоленской области

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (Ф.И.О.)

«\_\_»\_\_\_\_\_\_\_\_\_\_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 (подпись) (Фамилия И.О.)

пользователя АРМ заявителя)

 Приложение №4

к распоряжению Администрации

Усвятского сельского поселения

Дорогобужского района

Смоленской области

от 06.08.2019 г. № 88-р

**ИНСТРУКЦИЯ**

**по восстановлению связи в случае компрометации действующих ключей к СКЗИ Администрации Усвятского сельского поселения Дорогобужского района Смоленской области**

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 №5

к распоряжению Администрации

Усвятского сельского поселения

Дорогобужского района

Смоленской области

от 06.08.2019 г. № 88-р

**Состав**

**комиссии по допуску пользователей к самостоятельной работе с СКЗИ а Администрации Усвятского сельского поселения Дорогобужского района Смоленской области**

Председатель комиссии:

- Глава муниципального образования Усвятское сельское поселение

 Дорогобужского района Смоленской области – Павликов Леонид Петрович

Члены комиссии:

- главный специалист – Панскова Галина Анатольевна;

- ведущий специалист – Савенкова Анна Олеговна;

- специалист 1-й категории – Панёва Раиса Ивановна.