ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ КОМИ "РЕСПУБЛИКАНСКОЕ УЧРЕЖДЕНИЕ ТЕХНИЧЕСКОЙ ИНВЕНТАРИЗАЦИИ И КАДАСТРОВОЙ ОЦЕНКИ"

167000, Сыктывкар, ул. Карла Марса,197

П Р И К А З

«25» июля 2017 г. № 19

«Об утверждении Положения об обработке и защите Персональных данных в государственном бюджетном учреждении Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки»»

П Р И К А З Ы В А Ю:

1. Утвердить Положение об обработке и защите персональных данных в Государственном бюджетном учреждении Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки».
2. Главному юрисконсульту Пятовой Л.Г. ознакомить с Положением об обработке и защите персональных данных работников Государственного бюджетного учреждения Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки».
3. Назначить ответственным должностным лицом по обработке и защите персональных данных главного юрисконсульта Пятову Л.Г.
4. Контроль за исполнением данного приказа оставляю за собой.

Директор Е.Ю.Геттих

УТВЕРЖДЕНО
приказом директора
ГБУ РК «РУТИКО»
от 25 июля 2017 г. № 19
(приложение № 1)

ПОЛОЖЕНИЕ

об обработке и защите персональных данных в Государственном бюджетном учреждении Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки»

г.Сыктывкар

I. Общие положения

1.1. Положение об обработке и защите персональных данных в Государственном бюджетном учреждении Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки» (далее - Положение) определяет цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в Государственном бюджетном учреждении Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки» (далее - Учреждение).

1.2. Настоящее Положение определяет политику Учреждения как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

1.3. Настоящее Положение разработано в соответствии с Трудовым кодексом Российской Федерации, Кодексом Российской Федерации об административных правонарушениях, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных»), Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 2 сентября 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (далее - Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации»), постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 6 июля 2008 года № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» (зарегистрирован Министерством юстиции Российской Федерации 3 апреля 2008 г., регистрационный № 11462).

1.4. Обработка персональных данных в Учреждении осуществляется с соблюдением принципов и условий, предусмотренных настоящим Положением и законодательством Российской Федерации в области персональных данных.

1.5. Понятия, используемые в настоящем Положении:

- **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

- **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

- **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

- **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- **конфиденциальность персональных данных** - обязательное для соблюдения получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

II. Условия и порядок обработки персональных данных работников Учреждения

2.1. Персональные данные работников Учреждения обрабатываются в целях обеспечения кадровой работы, в том числе в целях содействия работнику в исполнении трудовой функции, обучении и должностном росте, учета результатов исполнения должностных обязанностей, обеспечения личной безопасности работников Учреждения, и членов их семьи, обеспечения установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества.

2.2. В целях, указанных в пункте 2.1 настоящего Положения, обрабатываются следующие категории персональных данных работников Учреждения:

2.2.1. фамилия, имя, отчество (последнее при наличии), дата и место рождения, гражданство;

2.2.2. сведения о стаже и трудовой деятельности;

2.2.3. семейное положение, состав семьи и сведения о близких родственниках;

2.2.4. сведения о месте регистрации и месте фактического проживания, номер телефона;

2.2.5. данные паспорта гражданина РФ и заграничного паспорта;

2.2.6. реквизиты страхового свидетельства обязательного пенсионнего страхования;

2.2.7. ИНН;

2.2.8. номер полиса обязательного медицинского страхования;

2.2.9. сведения с предыдущего места работы о доходах;

2.2.10.сведения о проведении служебных проверок и наложении дисциплинарных взысканий (вид взыскания, основание, дата снятия взыскания);

2.2.11. сведения о трудовом договоре;

2.2.12. сведения о должностном окладе, доплатах;

2.2.13. номер расчетного счета, номер банковской карты;

2.2.14. данные о награждении государственными и ведомственными наградами, иными наградами;

2.2.15. сведения о воинском учете и реквизиты документов воинского учета;

2.2.16. реквизиты свидетельства государственной регистрации актов гражданского состояния;

2.2.17. информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

2.2.18. сведения о профессиональном образовании (уровень образования, наименование образовательного учебного заведения, год окончания, дата выдачи диплома; номер диплома; специальность, квалификация);

2.2.19. иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 2.1 настоящего Положения.

2.3. Обработка персональных данных осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 2.1 настоящего Положения, в соответствии с пунктом 2 части 1 статьи 6 Федерального закона «О персональных данных» и положениями Трудового кодекса Российской Федерации.

2.4. Обработка специальных категорий персональных данных работников Учреждения не осуществляется.

2.5. Обработка персональных данных работников осуществляется при условии получения согласия указанных лиц в следующих случаях:

2.5.1. при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации;

2.5.2. при трансграничной передаче персональных данных;

2.5.3. при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

2.6. В случаях, предусмотренных пунктом 2.5 настоящего Положения, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

2.7. Обработка персональных данных работников Учреждения осуществляется специалистом по кадрам, главным бухгалтером, его заместителем, и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.8. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных работников Учреждения осуществляется путем:

2.8.1. получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные предоставляемые документы);

2.8.2. копирования оригиналов документов;

2.8.3. внесения сведений в учетные формы (на бумажных и электронных носителях);

2.8.4. формирования персональных данных в ходе кадровой, бухгалтерской работы;

2.8.5. внесения персональных данных в информационные системы Учреждения.

2.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от работников Учреждения. Работник Учреждения обязан передавать достоверные персональные данные в полном объеме, а в случае их изменения уведомлять учреждение в письменной форме.

2.10. В случае возникновения необходимости получения персональных данных работников Учреждения у третьей стороны, следует известить об этом работника Учреждения заранее, получить письменное согласие и сообщить о целях, предполагаемых источниках и способах получения персональных данных.

2.11. Запрещается получать, обрабатывать и приобщать к личному делу работника Учреждения персональные данные, не предусмотренные пунктом 2.2 настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.12. Персональные данные не могут быть использованы в целях причинения

имущественного и/или морального вреда гражданам, затруднения реализации прав и свобод граждан.

2.13. При сборе персональных данных специалист по кадрам, осуществляющий сбор (получение) персональных данных непосредственно от работников Учреждения обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

2.14. Передача (распространение, предоставление) и использование персональных данных работников Учреждения осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

2.15. В целях информационного обеспечения в Учреждении создаются общедоступные источники персональных данных, в том числе справочники (телефонные). В общедоступные источники персональных данных включаются: фамилия, имя, отчество, наименование обособленного подразделения (отдела), должность, номера контактных телефонов, адреса электронной почты и иные персональные данные, сообщаемые субъектом персональных данных, которые получают статус общедоступных. Запрещается размещать персональные данные субъекта, которые не получили статус общедоступных, в информационно-телекоммуникационной сети Интернет без получения устного или письменного согласия субъекта персональных данных.

2.16. Передача, хранение и доступ к персональным данным работников Учреждения.

2.16.1. Информация, относящаяся к персональным данным работника Учреждения, храниться в личном деле работника. Личные дела хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела хранятся в специально отведенной секции сейфа или иного запираемого шкафа, обеспечивающего защиту от несанкционированного доступа.

2.16.2. При передаче персональных данных работника оператор обязан соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать требования конфиденциальности;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

2.16.3. Внутренний доступ к персональным данным работника, в целях выполнения служебных обязанностей, имеют следующие работники Учреждения:

- директор;
- заместитель директора по кадастровой оценке;
- главный юрисконсульт;
- главный бухгалтер;
- заместитель главного бухгалтера;
- главный экономист;
- непосредственные руководители по направлению деятельности (доступ к персональным данным сотрудников, непосредственно находящихся в подчинении);
- непосредственно субъект персональных данных.

III. Условия и порядок обработки персональных данных лиц, не являющихся работниками Учреждения

3.1. Персональные данные лиц, не являющихся работниками Учреждения обрабатываются в целях соблюдения законодательства Российской Федерации в сфере кадастровой деятельности, деятельности по технической инвентаризации, государственной кадастровой оценке и реализации полномочий, возложенных на Учреждение в этой области.

3.2. В целях, указанных в пункте 3.1 настоящего Положения, обрабатываются следующие категории персональных данных лиц, не являющихся работниками Учреждения:

3.2.1. фамилия, имя, отчество (последнее при наличии), дата рождения;

3.2.2. сведения о месте регистрации и месте фактического проживания, номер телефона;

3.2.3. данные паспорта гражданина РФ;

3.2.4. номер расчетного счета, номер банковской карты;

3.2.5. СНИЛС;

3.2.6. иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 3.1 настоящего Положения.

3.3. Обработка персональных данных осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 3.1 настоящего Положения, в соответствии с пунктом 5 части 1 статьи 6 Федерального закона «О персональных данных».

3.4. Обработка персональных данных лиц, не являющихся работниками Учреждения осуществляется должностными лицами, указанными в п.2.16.3., и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

3.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных лиц, не являющихся работниками Учреждения осуществляется путем:

3.5.1. получения оригиналов необходимых документов;

3.5.2. копирования оригиналов документов;

3.5.3. внесения сведений в учетные формы (на бумажных и электронных носителях);

3.5.4. формирования персональных данных в ходе работы по организации учета и сверки;

3.5.5. внесения персональных данных в информационные системы Учреждения.

3.6. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно субъекта персональных данных, вступившего с Учреждением в гражданско-правовые отношения.

3.7. В случае возникновения необходимости получения персональных данных лиц, не являющихся работниками Учреждения у третьей стороны, следует известить об этом заранее, получить письменное согласие и сообщить о целях, предполагаемых источниках и способах получения персональных данных.

3.8. Запрещается получать, обрабатывать персональные данные, не предусмотренные пунктом 3.2 настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

IV. Условия и порядок обработки персональных данных субъектов в связи с организацией приема граждан, обеспечения своевременного и в полном объеме рассмотрения устных и письменных обращений граждан

4.1. В Учреждении обработка персональных данных физических лиц осуществляется в целях организация приема граждан, обеспечения своевременного и в полном объеме рассмотрения устных и письменных обращений граждан.

4.2. Персональные данные граждан, обратившихся в Учреждение лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением заявителей о результатах рассмотрения.

В соответствии с законодательством Российской Федерации в Учреждении подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан и лиц без гражданства.

4.3. В рамках рассмотрения обращений граждан подлежат обработке следующие персональные данные заявителей:

4.3.1. фамилия, имя, отчество (последнее при наличии);

4.3.2. почтовый адрес;

4.3.3. адрес электронной почты;

4.3.4. указанный в обращении контактный телефон;

4.3.5. иные персональные данные, указанные заявителем в обращении (жалобе), а также ставшие известными в ходе личного приема или в процессе рассмотрения поступившего обращения.

4.4. Обработка персональных данных, необходимых в связи с организацией приема граждан, обеспечения своевременного и в полном объеме рассмотрения устных и письменных обращений граждан осуществляется без согласия субъектов персональных данных в соответствии с пунктом 4 части 1 статьи 6 Федерального закона «О персональных данных», Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации».

4.5. Передача (распространение, предоставление) и использование персональных данных заявителей (субъектов персональных данных) осуществляется Учреждением лишь в случаях и в порядке, предусмотренных федеральными законами.

V. Порядок обработки персональных данных субъектов персональных данных в информационных системах

5.1. Обработка персональных данных в Учреждении осуществляется:

5.1.1. В информационной системе ПК «СЭД», «1С: Предприятие», ПК «СВОД-Смарт» (мониторинг зарплаты), «Гуляев Е.Ю.:зарплата», Налогоплательщик ЮЛ, Документы ПУ-6;

5.1.2. В информационной системе АС «Архив-БТИ», ПО «Полигон».

5.1.3. На автоматизированном рабочем месте главного юрисконсульта, ответственного за ведение кадрового делопроизводства.

5.2. Информационная система «1С: Предприятие» содержит персональные данные работников Учреждения и физических лиц, являющихся стороной гражданско-правовых договоров, заключаемых Учреждением, и включает:

5.2.1. фамилию, имя, отчество субъекта персональных данных (последнее при наличии);

5.2.2. дату рождения субъекта персональных данных;

5.2.3. место рождения субъекта персональных данных;

5.2.4. серию и номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе;

5.2.5. адрес места жительства субъекта персональных данных;

5.2.6. почтовый адрес субъекта персональных данных;

5.2.7. телефон субъекта персональных данных;

5.2.8. ИНН субъекта персональных данных;

5.2.9. табельный номер субъекта персональных данных;

5.2.10. должность субъекта персональных данных;

5.2.11. номер приказа и дату приема на работу (увольнения) субъекта персональных данных.

5.3. Автоматизированное рабочее место главного юрисконсульта, ответственного за ведение кадрового делопроизводства, предполагает обработку персональных данных работников Учреждения, предусмотренных пунктом 2.2 настоящего Положения.

5.4. Классификация информационных систем персональных данных, указанных в пункте 5.1 настоящего Положения, осуществляется в порядке, установленном законодательством Российской Федерации.

5.5. Работникам Учреждения, имеющим право осуществлять обработку персональных данных в информационных системах Учреждения, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе.

Информация вносится в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

5.6. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Учреждения, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

5.6.1. определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения;

5.6.2. применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

5.6.3. оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5.6.4. учет машинных носителей персональных данных;

5.6.5. обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

5.6.6. восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;

5.6.7. установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных Учреждения, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных Учреждения;

5.6.8. контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

Меры конфиденциальности при обработке персональных данных распространяются как на бумажные, так и на автоматизированные (электронные) носители информации.

5.7. Администратор безопасности в Учреждения, организует и контролирует ведение учета материальных носителей персональных данных.

5.8. Администратор безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения, должен обеспечить:

5.8.1. своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных в Учреждения и руководителя Учреждения;

5.8.2. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

5.8.3. возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5.8.4. постоянный контроль за обеспечением уровня защищенности персональных данных;

5.8.5. знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

5.8.6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

5.8.7. при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;

5.9. Обмен персональными данными при их обработке в информационных системах персональных данных Учреждения осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

5.10. Доступ работников Учреждения к персональным данным, находящимся в информационных системах персональных данных, предусматривает обязательное прохождение процедуры идентификации и аутентификации.

5.11. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных Учреждения, уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

VI. Сроки обработки и хранения персональных данных

6.1. Сроки обработки и хранения персональных данных работников Учреждения определяются в соответствии с законодательством Российской Федерации. С учетом положений законодательства Российской Федерации, устанавливаются следующие сроки обработки и хранения персональных данных работников:

6.1.1. Персональные данные, содержащиеся в приказах по личному составу (о приеме, о переводе, об увольнении, об установлении надбавок), подлежат хранению в Учреждении в течение трех лет, с последующим формированием и передачей указанных документов в архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение 75 лет.

6.1.2. Персональные данные, содержащиеся в личных делах работников, хранятся в Учреждении в течение десяти лет, с последующим формированием и передачей указанных документов в архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение 75 лет.

6.1.3. Персональные данные, содержащиеся в приказах о поощрениях, материальной помощи работников подлежат хранению в течение трех лет в Учреждении с последующим формированием и передачей указанных документов в архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение 75 лет.

6.1.4. Персональные данные, содержащиеся в приказах о предоставлении отпусков, о краткосрочных внутрироссийских и зарубежных командировках, о дисциплинарных взысканиях работников, подлежат хранению в Учреждении в течение пяти лет, с последующим уничтожением.

6.1.5. Персональные данные, содержащиеся в документах, формируемых в результате выполнения технической инвентаризации хранятся в Учреждении постоянно.

6.1.6. Сроки обработки и хранения персональных данных, предоставляемых субъектами персональных данных в Учреждение в связи с организацией личного приема и рассмотрением обращений, в том числе обращений в форме электронного документа, определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

6.2. Персональные данные, предоставляемые субъектами на бумажном носителе хранятся на бумажных носителях в Учреждения, у должностных лиц, осуществивших прием документов, в соответствии с исполнением должностных обязанностей.

6.3. Персональные данные при их обработке, осуществляемой без использования

средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

6.4. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящим Положением.

6.5. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют должностные лица, осуществляющие обработку персональных данных.

6.6. Срок хранения персональных данных, внесенных в информационные системы персональных данных Учреждения, указанные в пункте 5.1 настоящего Положения, должен соответствовать сроку хранения бумажных оригиналов.

VII. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

7.1. Специалист Учреждения, ответственный за архивирование документов, осуществляет систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

7.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании экспертной комиссии Учреждения. По итогам заседания составляются протокол и Акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами экспертной комиссии Учреждения.

7.3. Документы, содержащие персональные данные, подлежат уничтожению путем сжигания или химического уничтожения.

7.4. Уничтожение, по окончании срока обработки персональных данных на электронных носителях, производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

VIII. Рассмотрение запросов субъектов персональных данных или их представителей

8.1. Работники Учреждения, а также граждане, персональные данные которых обрабатываются в Учреждении, имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

8.1.1. подтверждение факта обработки персональных данных в Учреждении;

8.1.2. правовые основания и цели обработки персональных данных;

8.1.3. применяемые в Учреждении способы обработки персональных данных;

8.1.4. наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением или на основании федерального закона;

8.1.5. обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

8.1.6. сроки обработки персональных данных, в том числе сроки их хранения в Учреждении;

8.1.7. порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных

данных;

8.1.8. информацию об осуществленной или предполагаемой трансграничной передаче данных;

8.1.9. наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такой организации или лицу;

8.1.10. иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.

8.2. Лица, указанные в пункте 8.1 настоящего Положения (далее - субъекты персональных данных), вправе требовать от Учреждения уточнения их персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.3. Сведения, указанные в подпунктах 8.1.1 - 8.1.10 пункта 8.1 настоящего Положения, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

8.4. Сведения, указанные в подпунктах 8.1.1 - 8.1.10 пункта 8.1 настоящего Положения, предоставляются субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать:

8.4.1. номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

8.4.2. сведения, подтверждающие участие субъекта персональных данных в правоотношениях с Учреждениям, либо сведения, иным образом подтверждающие факт обработки персональных данных в Учреждении, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8.5. В случае, если сведения, указанные в подпунктах 8.1.1 - 8.1.10 пункта 8.1 настоящего Положения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Учреждение или направить повторный запрос в целях получения указанных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

8.6. Субъект персональных данных вправе обратиться повторно в Учреждение или направить повторный запрос в целях получения сведений, указанных в подпунктах 8.1.1 - 8.1.10 пункта 8.1 настоящего Положения, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 8.5 настоящего Положения, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 8.4 настоящего Положения, должен содержать обоснование направления повторного запроса.

8.7. Учреждение вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 8.5 и 8.6 настоящего Положения. Такой отказ должен быть мотивированным.

8.8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

IX. Лицо, ответственное за организацию обработки персональных данных в Учреждении

9.1. Ответственный за организацию обработки персональных данных в Учреждения (далее - ответственный за обработку персональных данных) назначается руководителем из числа работников Учреждения.

9.2. Ответственный за обработку персональных данных в своей работе руководствуется законодательством Российской Федерации в области персональных данных и настоящим Положением.

9.3. Ответственный за обработку персональных данных обязан:

9.3.1. организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в Учреждении от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

9.3.2. осуществлять внутренний контроль за соблюдением работниками Учреждения требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

9.3.3. доводить до сведения работников Учреждения положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

9.3.4. организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов в Учреждении. Обращения и запросы субъектов персональных данных рассматривает должностное лицо, осуществляющее их обработку;

9.3.5. в случае нарушения в Учреждении требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

9.4. Ответственный за обработку персональных данных вправе:

9.4.1. иметь доступ к информации, касающейся обработки персональных данных в Учреждении и включающей:

- цели обработки персональных данных;
- категории обрабатываемых персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовые основания обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых в Учреждения способов обработки персональных данных;
- описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- дату начала обработки персональных данных;
- срок или условия прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;

9.4.2. привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в Учреждении, иных работников с возложением на

них соответствующих обязанностей и закреплением ответственности.

X. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

10.1. Каждый работник Учреждения, получающий для работы документ, содержащий конфиденциальную информацию, в том числе персональные данные, несет персональную ответственность за сохранность носителя и информации.

10.2. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, привлекаются к ответственности в порядке, установленном законодательством Российской Федерации.

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ КОМИ «РЕСПУБЛИКАНСКОЕ УЧРЕЖДЕНИЕ ТЕХНИЧЕСКОЙ ИНВЕНТАРИЗАЦИИ И КАДАСТРОВОЙ ОЦЕНКИ»

ОРГН 1171101004128, ИНН/КПП 1101157842/110101001

ПРИКАЗ

11.04.2017г. № 12-од

г.Сыктывкар

Об утверждении перечня пользователей средств криптографической защиты информации

В целях исполнения требований п.19 «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 от 13 июня 2001г. №152 и на основании Заключений о допуске пользователя к самостоятельной работе сосредствами криптографической защиты информации (СКЗИ)

ПРИКАЗЫВАЮ:

1. Утвердить следующий перечень пользователей СКЗИ:

№ п/п	Фамилия Имя Отчество	Должность	Назначение СКЗИ (для работы в ГИС, бухгалтерских системах или государственных сайтах)	Наименование СКЗИ (ViPNetClient, КриптоПро, электронная подпись)	От кого получены СКЗИ *
1	Геттих Елена Юрьевна	директор	Для работы на zakupki.gov.ru как заказчик по 44-ФЗ	КрипоПро, электронная подпись	УЦ Федерального казначейства
2	Геттих Елена Юрьевна	директор	Для работы на электронных торговых площадках как поставщик	КрипоПро электронная подпись	ЗАО ПФ «СКБ Контур»
3	Соловьев Сергей Владимирович	И.о.главного бухгалтера	Для работы в бухгалтерских системах, bus.gov.ru	КрипоПро электронная подпись	ГАУ РК «ЦИТ»
4	Демина Ольга Александровна	Главный экономист	Для работы в АЦК планирование	планируется КрипоПро электронная подпись	ГАУ РК «ЦИТ»
5	Ли Наталья Николаевна	Руководитель группы по кадастровым	Для работы в программах Полигон	КрипоПро, электронная подпись	Технокад-Экспресс

		работам			
6	Тиранова Ольга Николаевна	Кадастровый инженер	Для работы в программах Полигон	КрипоПро, электронная подпись	Технокад-Экспресс
7	Князев Василий Васильевич	Кадастровый инженер	Для работы в программах Полигон	КрипоПро, электронная подпись	Технокад-Экспресс
8	Пятова Людмила Геннадьевна	Главный юрисконсульт	Планируется ГИС СЭД, информационный ресурс ССТУ.РФ	КриптоПро	ЗАО ПФ «СКБ Контур»

2. Контроль за исполнением настоящего приказа возложить на Пятову Людмилу Геннадьевну.

Директор Е.Ю.Геттих

* ГАУ РК «ЦИТ», ГБУ Республики Коми «ЦБИ», Управление Федерального казначейства по Республике Коми либо иные организации, распространяющие СКЗИ.

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ КОМИ «РЕСПУБЛИКАНСКОЕ УЧРЕЖДЕНИЕ ТЕХНИЧЕСКОЙ ИНВЕНТАРИЗАЦИИ И КАДАСТРОВОЙ ОЦЕНКИ»

ОРГН 1171101004128, ИНН/КПП 1101157842/110101001

ПРИКАЗ

«11» 04 2017 года г. Сыктывкар № 13-од

«Об утверждении инструкции об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные в информационной системе персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные информационных систем персональных данных (ИСПДн) Государственного бюджетного учреждения Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки» (ГБУ РК «РУТИКО»).
2. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Е.Ю.Геттих

УТВЕРЖДЕНА
приказом директора
ГБУ РК «РУТИКО»
от _____ №_____

ИНСТРУКЦИЯ
об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные в информационной системе персональных данных

1. Настоящая Инструкция устанавливает организацию учета, хранения и выдачи машинных носителей, содержащих персональные данные информационных систем персональных данных (ИСПДн) Государственного бюджетного учреждения Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки» (ГБУ РК «РУТИКО»).

2. Учет, хранение и выдачу машинных носителей персональных данных осуществляет ответственный за организацию обработки персональных данных (далее - Ответственный). При увольнении сотрудника, ответственного за учет, хранение и выдачу машинных носителей персональных данных, составляется акт приема-сдачи этих документов, который утверждается директором ГБУ РК «РУТИКО».

3. Все находящиеся на хранении и в обращении машинные носители персональных данных (далее - носители) подлежат учёту. Учет всех видов и типов носителей производится в Журнале учета машинных носителей, содержащих персональные данные.

Каждый носитель должен иметь этикетку, на которой указывается его уникальный учетный номер. На несъемной части упаковки носителя ПДн указывается:

- учетный номер;
- отметка «Персональные данные»;
- дата регистрации (день, месяц, год);
- ФИО, должность, подпись сотрудника, выполнившего учет.

4. Пользователи ИСПДн получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в Журнале учета машинных носителей, содержащих персональные данные. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в Журнале учета машинных носителей, содержащих персональные данные.

5. Хранение носителей осуществляется в условиях, исключающих несанкционированное копирование, изменение или уничтожение персональных данных, а также хищение носителей. Носители должны храниться в служебных помещениях, в металлическом хранилище (сейфе) в установленном порядке. Запрещается хранить машинные носители персональных данных вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

6. В случае утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений, немедленно ставится в известность Ответственный. Соответствующие отметки вносятся в Журнале учета машинных носителей, содержащих персональные данные.

7. Носители, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. По результатам уничтожения носителей составляется Акт уничтожения машинных носителей персональных данных (приложение № 1).

8. При передаче средств вычислительной техники ИСПДн сторонним организациям для проведения ремонтно-восстановительных или иных работ, несъемные машинные носители изымаются из состава средств вычислительной техники.

9. Ответственность за выполнение правил эксплуатации машинных носителей персональных данных при выполнении непосредственных работ с носителями несет пользователь ИСПДн.

10. Контроль выполнения пользователями установленных правил эксплуатации машинных носителей персональных данных, осуществляет Ответственный.

Приложение № 1
к инструкции об организации учета,
хранения и выдачи машинных
носителей

АКТ
уничтожения машинных носителей персональных данных

Комиссия, наделенная полномочиями приказом от _____ № _____ в составе: _____
(должности, Ф.И.О.)
провела отбор машинных носителей персональных данных, не подлежащих дальнейшему хранению:

N п/п	Дата	Учетный номер машинного носителя	Пояснения
1	2	3	4

Всего съемных носителей _____
(цифрами и прописью)

На машинных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные машинные носители уничтожены _____
путем (разрезания, демонтажа и т.п.), _____
измельчены и сданы для уничтожения предприятию по утилизации вторичного сырья _____
(наименование предприятия) Дата

Председатель комиссии Подпись Дата

Члены комиссии
(Ф.И.О.) Подпись Дата

Лист ознакомления с «Инструкцией об организации учета, хранения и выдачи машинных носителей»

№ п/п	ФИО	Должность	Подпись, дата

Государственное бюджетное учреждение Республики Коми
«Республиканское учреждение технической инвентаризации и кадастровой оценки»

УТВЕРЖДАЮ
Директор
_____ /_____
«__» _____ 2017 года

ЖУРНАЛ №___
учета машинных носителей, содержащих персональные данные

Журнал начат «__»_____ 201___года

Журнал завершен «__»_____20__ года

На ___ листах

г. Сыктывкар

№ п/п	Дата регистрационный номер	Учетный номер	Тип машинного носителя информации	Кол-во экз.	Номер экз.	Кол-во ПДн в экземпляре	Расписка в получении, отметка об отправке	Расписка в обратном приеме

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ КОМИ «РЕСПУБЛИКАНСКОЕ УЧРЕЖДЕНИЕ ТЕХНИЧЕСКОЙ ИНВЕНТАРИЗАЦИИ И КАДАСТРОВОЙ ОЦЕНКИ»

ОРГН 1171101004128, ИНН/КПП 1101157842/110101001

ПРИКАЗ

«11» 04 2017 года г. Сыктывкар № 14-од

«О контролируемой зоне»

В соответствии со Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30.08.2002 № 282,

ПРИКАЗЫВАЮ:

1. Определить контролируемую зону ограждающей конструкции охраняемого здания Государственного бюджетного учреждения Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки» в соответствии с приложением № 1.
2. Определить, что организацию охраны контролируемой зоны осуществляет арендодатель – ООО «Промжилстрой», на основании договора с ООО ЧОО «Группа Компаний «Конфидент».
3. Утвердить Инструкцию по охране контролируемой зоны Государственного бюджетного учреждения Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки» (приложение № 2).
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Е.Ю.Геттих

УТВЕРЖДЕНО
приказом директора ГБУ РК
«РУТИКО»
«11» 04 2017г. №14-од
(приложение № 1)

ОПИСАНИЕ
контролируемой зоны Государственного бюджетного учреждения Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки»

Контролируемая зона — это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей, а также транспортных, технических и иных материальных средств.

Определить контролируемую зону проходящую по внутреннему периметру ограждающих конструкций охраняемого здания, принадлежащего ООО «Промжилстрой», находящемуся по адресу г.Сыктывкар, ул.Карла Маркса, д.197, 2-й этаж:

рис.1.контролируемая зона (схема)

УТВЕРЖДЕНА
приказом руководителя Учреждения
от «14» 04 2017 г № 1409
(приложение № 2)

ИНСТРУКЦИЯ
по организации охраны контролируемой зоны в Учреждении

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция разработана с целью организации охраны контролируемой зоны.
1.2. Граница контролируемой зоны утверждается приказом руководителя Учреждения.
1.3. Контролируемая зона – это территория объекта, на которой исключено неконтролируемое пребывание лиц.
1.4. Настоящая инструкция обязательна при взаимодействии с дежурными вахтерами ООО «Промжилстрой», ответственными за организацию охраны контролируемой зоны.

II. ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА

2.1. Учреждение располагается по адресу: г.Сыктывкар, ул.Карла Маркса, д.197, 2-й этаж, кабинеты №№205, 206, 207, 208, 209.
2.2. На территории Учреждения располагаются следующие объекты: ООО «Промжилстрой», нотариус Микушева Л.И., КПК «Фонд скорой финансовой помощи», ООО «Энергоресурс», ООО «Жилье», ООО «Управление строительства», НКО «Фемида», ООО «Консульт-Эффект», ООО «Стройторгсервис».
2.3. Второй этаж имеет 2 выхода –лестничные клетки, 1 лифт. Здание имеет 3 выхода.
2.4. Количество сотрудников Учреждения 17.

III. ОРГАНИЗАЦИЯ ОХРАНЫ КОНТРОЛИРУЕМОЙ ЗОНЫ

3.1. Обход второго этажа здания осуществляется дежурным вахтером ООО «Промжилстрой». По периметру этажа установлены камеры видеонаблюдения, с выходом на пульт дежурного вахтера на 1-м этаже здания. Охранная сигнализация обеспечивается ООО «ЧОП «Группа компаний «Конфидент» по договору с ООО «Промжилстрой».
3.2. В ночное время, в выходные и нерабочие праздничные дни обход осуществляется дежурным вахтером ООО «Промжилстрой».
3.3. При обходе дежурный вахтер осматривает этаж по периметру на предмет их целостности коробов, кабель-каналов, кабельных

лотков, кабельных лестничных лотков кабелей локально-вычислительных сетей (далее – ЛВС) проложенных по всему этажу.

3.4. Доступ посторонних лиц к коробам, кабель-каналам, кабельных лотков, кабельных лестничных лотков кабелей ЛВС исключен.

3.5. При обнаружении внешнего повреждения короба, кабель-канала, кабельных лотков, кабельных лестничных лотков кабелей ЛВС, дежурный вахтер незамедлительно сообщает руководителю Учреждения, с указанием места повреждения, даты и времени обнаружения повреждения.

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ КОМИ «РЕСПУБЛИКАНСКОЕ УЧРЕЖДЕНИЕ ТЕХНИЧЕСКОЙ ИНВЕНТАРИЗАЦИИ И КАДАСТРОВОЙ ОЦЕНКИ»

ОРГН 1171101004128, ИНН/КПП 1101157842/110101001

ПРИКАЗ

«11» 04 2017 года г. Сыктывкар № 10-ОД

«Об утверждении списка лиц, допущенных к обработке персональных данных в информационных системах персональных данных Государственного бюджетного учреждения Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки»

ПРИКАЗЫВАЮ:

1. Назначить ответственным лицом за организацию обработки персональных данных главного юрисконсульта Государственного бюджетного учреждения Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки» Пятову Людмилу Геннадьевну.
2. Утвердить список лиц, допущенных к обработке персональных данных в информационных системах персональных данных Государственного бюджетного учреждения Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки» в соответствии с приложением № 1.
3. Утвердить разрешительную систему (матрицу доступа) к информационным (программным) ресурсам.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Е.Ю.Геттих

УТВЕРЖДЕН
приказом директора
ГБУ РК «РУТИКО»
от 24.04.2023 № 10
(приложение № 1)

Список лиц, допущенных к обработке персональных данных в информационных системах персональных данных Государственного бюджетного учреждения Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки»

Система электронного документооборота органов государственной власти Республики Коми

Таблица 1. Список лиц, допущенных к обработке ПДн в ИСПДн

№	Ф.И.О.	Должность	Роль
1.	Геттих Елена Юрьевна	Директор	Пользователь с правами записи
2.	Соловьев Сергей Владимирович	И.о.главного бухгалтера	Пользователь с правами записи
3.	Пятова Людмила Геннадьевна	Главный юрисконсульт	Пользователь с правами записи
4.	Демина Ольга Александровна	Главный экономист	Пользователь с правами записи

Актуальный перечень лиц, имеющих доступ к определенным категориям персональных данных, а также их полномочия можно получить у ответственного за организацию обработки персональных данных.

УТВЕРЖДАЮ

ДИРЕКТОР

ГБУ РК «РУТИКО»

_____ /Е.Ю.Геттих

«11» 04 2017 г.

РАЗРЕШИТЕЛЬНАЯ СИСТЕМА (МАТРИЦА) ДОСТУПА

к информационным (программным) ресурсам

Государственного бюджетного учреждения Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки»

2017г.

Матрица доступа к информационным (программным) ресурсам.

№ п/п	Фамилия пользователя	Имя компьютера в сети	Информационные системы
			СЭД
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
Место расположения информационных систем			ЦОД ГАУ РК «ЦИТ»

Условные обозначения:
A – полные права доступа;
R - чтение;
W - запись;
X - выполнение программ;
D - удаление.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«__» _____ 201____г.

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ КОМИ «РЕСПУБЛИКАНСКОЕ УЧРЕЖДЕНИЕ ТЕХНИЧЕСКОЙ ИНВЕНТАРИЗАЦИИ И КАДАСТРОВОЙ ОЦЕНКИ»

ОРГН 1171101004128, ИНН/КПП 1101157842/110101001

ПРИКАЗ

11.04.2017г. № 11-ОД

г.Сыктывкар

Об обращении со средствами криптографической защиты информации

В целях исполнения требований «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 от 13 июня 2001 г. №152,

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию работ по криптографической защите информации юрисконсульта Пятову Людмилу Геннадьевну;
2. Утвердить Инструкцию ответственного за организацию работ по криптографической защите информации (Приложение 1);
3. Ответственному за организацию работ по криптографической защите информации ознакомиться под роспись и руководствоваться в своей деятельности Инструкцией ответственного за организацию работ по криптографической защите информации;
4. Утвердить Инструкцию по обращению со средствами криптографической защиты информации (СКЗИ) (Приложение 2),
5. Ответственному за организацию работ по криптографической защите информации ознакомлять под роспись пользователей СКЗИ с Инструкцией по обращению с СКЗИ;
6. Пользователям, которым необходимо получить доступ к работе с СКЗИ, пройти обучение правилам работы с СКЗИ в форме тестирования на сайте ГАУ РК «ЦИТ»;
7. Утвердить Перечень пользователей СКЗИ (отдельным приказом в двух экземплярах);
8. Утвердить форму Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Приложение 3);
9. Утвердить форму Акта об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов (Приложение 4);
10. Утвердить формуЖурнала сдачи и приема экземпляров ключей от запираемых хранилищ (Приложение 5).
11. Настоящий Приказ подготовить в двух экземплярах.
12. В течение трех рабочих дней со дня подписания настоящего приказа направить в ГАУ РК «ЦИТ»

- экземпляр настоящего Приказа,
- экземпляр Приказа об утверждении Перечня пользователей СКЗИ,

13. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Е.Ю.Геттих

УТВЕРЖДЕНО
приказом директора ГБУ РК «РУТИКО»
от «11» июля 2017 года № 77-од
(Приложение 1)

Государственное бюджетное учреждение Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки»

ИНСТРУКЦИЯ

ответственного за организацию работ по криптографической защите информации

1. Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, ответственных за организацию работ по криптографической защите информации (далее – Ответственный) в организациях, которые осуществляют работы с применением средств криптографической защиты информации (СКЗИ) (далее – Организация).

Под Организацией в настоящей Инструкции понимаются органы государственной власти Республики Коми, подведомственные им организации, органы местного самоуправления Республики Коми, подведомственные им организации.

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и т.д.

Ответственный назначается приказом руководителя Организации из числа её работников.

СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

Функции по проведениюмероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации ограниченного доступа осуществляет Государственное автономное учреждение Республики Коми "Центр информационных технологий" (далее – ГАУ РК «ЦИТ»).

Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях «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 от 13 июня 2001 г. №152 (далее – Инструкция ФАПСИ от 13 июня 2001 г. №152), «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66, «Типовыми требованиями 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», утвержденными руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/6/6-622.

2. Термины и определения

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

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

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

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

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

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

Персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем Организации в рамках исполнения должностных обязанностей.

Пользователи СКЗИ – работники Организации, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

3. Порядок получения допуска пользователей к работе с СКЗИ

Для работы пользователей с СКЗИ в Организации необходимо реализовать ряд мероприятий:

1) Пользователям, которым необходимо получить доступ к работе с СКЗИ, пройти самостоятельное обучение правилам работы с СКЗИ и тестирование на знание этих правил на сайте ГАУ РК «ЦИТ» (http://www.test.cit.rkomi.ru);
2) Издать Приказ об утверждении перечня пользователей СКЗИ;
3) Утвердить Инструкцию по обращению с СКЗИ;
4) Ознакомить всех пользователей СКЗИ с Инструкцией по обращению с СКЗИ под роспись.
5) По факту подготовки незамедлительно направить в ГАУ РК «ЦИТ» экземпляр Приказа об обращении с СКЗИ (без приложений), экземпляр Приказа об утверждении перечня пользователей СКЗИ.

Контроль над реализацией данных мероприятий возлагается на Ответственного.

4. Обязанности Ответственного

При решении всех вопросов, связанных с обеспечением в Организации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, Ответственный должен руководствоваться Инструкцией по обращению с СКЗИ, которая утверждается Приказом об обращении с СКЗИ.

На Ответственного возлагается проведение следующих мероприятий:

1) Вести Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
2) Вести учет переданных от ГАУ РК «ЦИТ» актов об установке и настройке СЗИ;
3) Вести учет переданных от ГАУ РК «ЦИТ» лицензий на право использования СКЗИ и соответствующих им Актов приема-передачи;
4) Принять СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
5) Письменно уведомлять ГАУ РК «ЦИТ» в течение трех рабочих днейоб изменениях или увольнениях пользователей СКЗИ;
6) Осуществлять ежегодную проверку журнала учета СКЗИ, перечня пользователей СКЗИ и иных документов и письменно уведомлять ГАУ РК «ЦИТ» о результатах проверки в срок не позднее «01» февраля года, следующего за отчетным;
7) Сообщать в ГАУ РК «ЦИТ» о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним.

Ответственный обязан

1) Не разглашать информацию ограниченного доступа, к которой он допущен, в том числе сведения о криптоключах;
2) Сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;
3) Соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;
4) Контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ;
5) Немедленно уведомлять ГАУ РК «ЦИТ» о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах компрометации криптоключей, которые могут привести к разглашению информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;
6) Незамедлительно принимать меры по локализации последствий компрометации защищаемых сведений конфиденциального характера;
7) Не допускать ввод одного номера лицензии на право использования СКЗИ более чем на одно рабочее место.
8) Обеспечивать централизованное хранение в специально выделенном хранилище дубликатов ключей от запираемых хранилищ пользователей ключевых носителей СКЗИ, а также их учет по Журналу сдачи и приема экземпляров ключей от запираемых хранилищ. Дубликат ключа хранится в закрытом конверте, на котором указываются фамилия,имя,отчество пользователя СКЗИ, номер помещения, в котором находится хранилище, и инвентарный номер хранилища.

5. Права Ответственного

В рамках исполнения возложенных на него обязанностей, Ответственный имеет право

1) Требовать от пользователей СКЗИ соблюдения положений Инструкции по обращению с СКЗИ;
2) Обращаться к руководителю Организации с требованием прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;
3) Инициировать проведение служебных расследований по фактам нарушения в Организации порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

6. Порядок передачи обязанностей при смене Ответственного

При смене Ответственного должны быть внесены соответствующие изменения в Приказ об обращении с СКЗИ. Вновь назначенный Ответственный должен быть ознакомлен под роспись с настоящей Инструкцией и приступить к исполнению возложенных на него обязанностей.

7. Заключительные положения

Ознакомление с нормативными документами в области СКЗИ возможно на сайте ГАУ РК «ЦИТ» (http://www.test.cit.rkomi.ru).

Отправку всех необходимых документов осуществлять на адрес ГАУ РК «ЦИТ»: 167000, г. Сыктывкар, ул. Интернациональная, д. 108, оф. 227.

Телефон: (8212) 30-12-11.

Лист ознакомления

с Инструкцией ответственного за организацию работ

по криптографической защите информации

(утверждена приказом от «11» 04 2017 г. № 11-од)

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата

УТВЕРЖДЕНО
приказом директора ГБУ РК «РУТИКО»
от «11» 04 2017 года № 11-09
(Приложение 2)

Государственное бюджетное учреждение Республики Коми «Республиканское учреждение технической инвентаризации и кадастровой оценки»

ИНСТРУКЦИЯ

по обращению со средствами криптографической защиты информации

1. Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (СКЗИ) в организациях, которые осуществляют работы с применением СКЗИ (далее – Организация).

Под Организацией в настоящей Инструкции понимаются органы государственной власти Республики Коми, подведомственные им организации, органы местного самоуправления Республики Коми, подведомственные им организации.

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и т.д.

Под обращением с СКЗИ в настоящей Инструкции понимается проведение мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

Функции по проведению мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации ограниченного доступа осуществляет Государственное автономное учреждение Республики Коми "Центр информационных технологий" (далее – ГАУ РК «ЦИТ»).

Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях «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 от 13 июня 2001 г. №152 (далее – Инструкция ФАПСИ от 13 июня 2001 г. №152), «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66, «Типовыми требованиями 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», утвержденными руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/6/6-622.

2. Термины и определения

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

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

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

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

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

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

Персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем Организации в рамках исполнения должностных обязанностей.

Пользователи СКЗИ – работники Организации, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2. Работа с СКЗИ

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае, в организации должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

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

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

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) сотрудниками ГАУ

РК «ЦИТ» под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями СКЗИ должна быть санкционирована ГАУ РК «ЦИТ». Организация с согласия ГАУ РК «ЦИТ» может разрешить передачу СКЗИ, документации к ним, ключевых документов между допущенными к СКЗИ лицами по актам без обязательной отметки в журнале поэкземплярного учета.

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

3. Действия в случае компрометации ключей

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

К компрометации ключей относятся следующие события:

1) утрата носителей ключа;
2) утрата иных носителей ключа с последующим обнаружением;
3) увольнение сотрудников, имевших доступ к ключевой информации;
4) возникновение подозрений на утечку информации или ее искажение;
5) нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
6) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
7) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
8) доступ посторонних лиц к ключевой информации;
9) другие события утери доверия к ключевой документации.

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

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

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

4. Обязанности и ответственность лиц, допущенных к работе с СКЗИ

Лица, допущенные к работе с СКЗИ, обязаны

1) Не разглашать информацию ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;
2) Сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;
3) Соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;
4) Сообщать в ГАУ РК «ЦИТ» о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

5) Немедленно уведомлять ГАУ РК «ЦИТ» о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

6) В случае необходимости производить уничтожение криптоключей и ключевых документов в соответствии с требованиями пунктов 41-46 Инструкции ФАПСИ от 13 июня 2001 г. №152 и уведомлять об этом ГАУ РК «ЦИТ».

7) Не вводить номера лицензий на СКЗИ, уже вводимые на других АРМ;

8) По окончании рабочего дня убирать ключевые носители в запираемые шкафы, ящики столов или сейфы (далее – хранилища). Пользователь не имеет права без письменного указания Ответственного за организацию работ по криптографической защите передавать ключ от хранилища третьим лицам и несет ответственность за его сохранность. Дубликат ключа от хранилища необходимо передать Ответственному за организацию работ по криптографической защите с записью в Журнале сдачи и приема экземпляров ключей от запираемых хранилищ.

Лица, допущенные к работе с СКЗИ, отвечают за исполнение своих функциональных обязанностей и сохранность информации ограниченного доступа, которая стала ему известной вследствие исполнения им своих служебных обязанностей.

Ответственность лиц, допущенных к работе с СКЗИ, за неисполнение и (или) ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими инструкциями (Инструкция ответственного за организацию работ по криптографической защите информации, Инструкция пользователя СКЗИ), а также за разглашение информации ограниченного доступа, ставшей ему известной вследствие исполнения им своих служебных обязанностей, определяется действующим законодательством Российской Федерации и условиями трудового договора.

5. Заключительные положения

Контактная информация ГАУ РК «ЦИТ»:
Адрес: 167000, г. Сыктывкар, ул. Интернациональная, д. 108, оф. 227.
Телефон: (8212) 301-211
Сайт: http://www.test.cit.rkomi.ru/

Лист ознакомления

с Инструкцией по обращению со средствами

криптографической защиты информации

(утверждена приказом от «11» 04 20 17 г. №11-од)

№ п/п	ФИО	Должность	Подпись, дата

УТВЕРЖДЕНО
приказом директора ГБУ РК «РУТИКО»
от «11» 04 2017 года № 11-од
(Приложение 3)

Журнал поэкземплярного учета СКЗИ (форма)

Журнал начат «____» _____ 201__ г.

Журнал завершен «____» _____ 201__ г.

На _____ листах

№ п/п	Наименование СКЗИ	Лицензионный/серийный номер СКЗИ	Учетный номер дистрибутива СКЗИ	Отметка о получении		Отметка о подключении (установке СКЗИ)				Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов		Примечание
				Наименование организации, передавшей СКЗИ	Номер и дата документа, подтверждающего получение СКЗИ	Ф.И.О. пользователя СКЗИ	Ф.И.О. сотрудника, установившего СКЗИ	Дата подключения (установки) СКЗИ, расписка об установке	Инв. номер аппаратных средств,на которые установлены СКЗИ	Ф.И.О. сотрудника, производившего изъятие (уничтожение) СКЗИ	Дата изъятия (удаления) СКЗИ, расписка об уничтожении (удалении)	
1	2	3	4	5	6	7	8	9	10	11	12	13

УТВЕРЖДЕНО
приказом директора ГБУ РК «РУТИКО»
от «11» 07 2017 года № 11-00
(Приложение 4)

АКТ № _____ от «__» _____ 20__ г. (форма)
об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов

Комиссия сотрудников _____ в составе:
(название организации)
_____
_____
_____
произвела уничтожение криптографических ключей, содержащихся на ключевых носителях, и ключевых документов:

№	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего уничтожается ключей (документов)

Всего уничтожено _____ криптографических ключей на _____ ключевых носителях.

Уничтожение криптографических ключей выполнено путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Факт списания с учета ключевых носителей в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов **подтверждаю**:

Ответственный за организацию работ по криптографической защите информации _____/_____

Члены комиссии:

_____/_____
_____/_____
_____/_____

УТВЕРЖДЕНО
приказом директора ГБУ РК «РУТИКО»
от «11» 04 2017 года № 11-09
(Приложение 5)

Журнал сдачи и приема экземпляров ключей от запираемых хранилищ (форма)

Журнал начат «____» _____ 201__ г.

Журнал завершен «____» _____ 201__ г.

На _____ листах

№п/п	Дата и время сдачи	Номер хранилища, номер помещения, где расположено хранилище	Отметка о сдаче ключа		Отметка о приеме ключа	
			ФИО сдающего лица	Подпись сдающего лица	ФИО принимающего лица	Подпись принимающего лица
1	2	3	4	5	6	7