Приложение №1
к приказу от «16» декабря 2025 г. №315

У Т В Е Р Ж Д А Ю

Директор
Муниципального учреждения
«Дом культуры «Матыра»
_____ Л.Л. Черепахина
«16» декабря 2025 г.

МП

ИНСТРУКЦИЯ

Администратора информационной безопасности

Липецк 2025

1. Термины, определения и сокращения

Автоматизированная система (АС) – Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Автоматизированное рабочее место (АРМ) – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Администратор информационной безопасности – лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Безопасность информации [данных] – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Защита информации от несанкционированного доступа (ЗИ от НСД) – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защита информации от разглашения – защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Государственная информационная система (ГИС) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Носитель защищаемой информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Носитель информации (НИ) – материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин ("Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008)).

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

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 (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Оператор персональных данных – 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 (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Система защиты информации (СЗИ) – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Средство защиты информации (СрЗИ) – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

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 (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

2. Общие положения

2.1. Настоящая инструкция разработана на основании следующих нормативных документов:

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

2.1.2. Федеральный закон от 27 июня 2006 № 152-ФЗ «О персональных данных»;

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

2.1.4. Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

2.2. Инструкция определяет основные задачи, функции, обязанности, права и ответственность Администратора информационной безопасности информационной системы (далее –ИС) организации (далее – Организация).

2.1. Администратор информационной безопасности выполняет функции по обеспечению бесперебойного функционирования систем защиты.

2.2. Администратор информационной безопасности назначается приказом директором МУ «ДК «Матыра».

2.3. В своей деятельности Администратор информационной безопасности руководствуется требованиями действующих федеральных законов, общегосударственных и ведомственных нормативных документов по вопросам защиты конфиденциальной информации, в том числе персональных данных и обеспечивает их выполнение.

2.4. Настоящая Инструкция является дополнением к действующим регламентирующим документам по вопросам защиты информации в Организации и не исключает обязательного выполнения их требований.

3. **Основными задачами Администратора информационной безопасности являются:**

3.1. Осуществлять настройку технических и программных средств системы защиты информации в информационных системах (далее – СЗИ ИС).

3.2. Обеспечивать контроль работоспособности и проводить восстановление работоспособности средств защиты информации (далее - СрЗИ) и СЗИ ИС в целом в случае отказов (сбоев).

3.3. Проводить мероприятия по техническому (сервисному) обслуживанию средств защиты информации, входящих в состав ИС.

3.4. Разрабатывать таблицу разграничения доступа в ИС (далее - матрицу доступа): доступ к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа. Матрица разграничения доступа составляется как на электронном, так и на бумажном носителях

3.5. Участвовать в выявлении инцидентов, которые могут привести к сбоям или нарушению функционирования, или к возникновению новых угроз безопасности информации, и реагирование на них.

3.6. Осуществлять выявление (поиск), анализ и устранение уязвимостей.

4. **Обязанности Администратора информационной безопасности**

4.1. Осуществлять поэкземплярный учет средств защиты информации, эксплуатационной и технической документации к ним, в том числе используемых средств криптографической защиты информации, ключевых документов.

4.1.1 Осуществлять контроль за соблюдением условий использования средств криптографической защиты информации, установленных эксплуатационной и технической документацией на средства криптографической защиты информации в соответствии с «Инструкцией по обращению со средствами криптографической защиты».

4.1.2 Вести учет носителей информации, осуществлять их хранение, прием, выдачу, контролировать правильность их использования в соответствии с «Инструкцией по организации учета, использования и уничтожения машинных носителей информации».

4.1.3. Осуществлять настройку журналов регистрации событий информационной безопасности в программном обеспечении ИС и СЗИ, установленной в «Журнале учета инцидентов информационной безопасности».

4.1.4. Осуществлять выполнение требований парольной защиты в рамках своей компетенции.

4.1.5. Проводить обучение (инструктаж) пользователей правилам работы со средствами защиты информации, применяемыми в ИС.

4.1.6. Осуществлять ознакомление пользователей с:

- «Инструкцией пользователя…»;
- «Инструкцией по применению средств антивирусной защиты»;
- «Инструкцией по организации парольной защиты».

4.1.7. В ходе выполнения задач по управлению (администрированию) системой защиты информации обеспечивать:

- заведение и удаление учетных записей пользователей, управление полномочиями пользователей и поддержание правил разграничения доступа (Матрица разграничения доступа);
- блокирование, контроль использования, при необходимости, пересмотр и корректировка учетных записей пользователей;
- генерацию, смену и восстановление паролей пользователей в соответствии с «Инструкцией по организации парольной защиты»;
- управление средствами защиты информации, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации;
- порядок применения средств антивирусной защиты, а также порядок действий при обнаружении программных вирусов в соответствии с «Инструкций по применению средств антивирусной защиты»;
- установку обновлений программного обеспечения, включая программное обеспечение средств защиты информации;
- восстановление работоспособности средств защиты информации;
- анализ событий, связанных с защитой информации (далее – события безопасности), для выявления попыток несанкционированного доступа к защищаемым ресурсам;
- обеспечение использования для выявления (поиска) уязвимостей средств анализа защищенности, имеющих стандартизованные перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей (Политика (регламент) управления уязвимостями).

4.1.8. В ходе выполнения задач по выявлению и реагированию на инциденты в системе защиты информации обеспечивать:

- обнаружение и идентификацию инцидентов, в ом числе отказ в обслуживании, сбоев (перегрузок) в работе технических средств, программном обеспечении и средствах защиты информации, нарушений правил разграничения доступа, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих возникновению инцидентов;

- анализ инцидентов, определение источников и причин возникновения инцидентов, а также оценку их последствий;

- планирование и принятие мероприятий по предотвращению повторного возникновения инцидентов (Администратор информационной безопасности руководствуется Инструкцией по регистрации, выявлению и реагированию на инциденты).

4.1.9. Осуществлять установку (инсталляцию) только разрешенного к использованию в ИС программного обеспечения и (или) его компонентов.

4.1.10. В ходе выполнения задач по контролю за обеспечением уровня защищенности выполнять:

- контроль установки обновлений программного обеспечения;

- контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

- контроль состава технических средств, программного обеспечения и средств защиты информации;

- контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа.

4. 2. Администратору информационной безопасности запрещается:

4.2.1.Используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ее модификации, копирования, уничтожения.

4.2.2.Использовать ставшие доступные в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий.

4.2.3.Использовать в своих и в чьих-либо личных интересах информационные ресурсы, предоставлять такую возможность другим.

4.2.4.Выключать СЗИ без санкции руководства.

4.2.5.Передавать третьим лицам сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки.

4.2.6.Нарушать правила эксплуатации оборудования.

5. Права и ответственность Администратора информационной безопасности

5.1.Администратор информационной безопасности имеет право:

5.1.1.Получать доступ к программным и аппаратным средствам, средствам их защиты, а также просмотру прав доступа к ресурсам на рабочих станциях пользователей.

5.1.2.Контролировать действия пользователей выполнения инструкций по обеспечению безопасности и защите информации.

5.1.3.Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа (далее – НСД), утраты, порчи защищаемой информации и технических компонентов.

5.1.4.Производить анализ защищенности и попыток взлома системы защиты ИС путем применения специальных средств.

5.1.5.Вносить предложения руководству по совершенствованию мер защиты.

5.1.6.Требовать от руководства оказания содействия в исполнении своих должностных обязанностей и прав.

5.2.Администратор информационной безопасности несет ответственность за:

5.2.1. Программно-технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и автоматизированные системы обработки информации.

5.2.2. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим трудовым законодательством Российской Федерации.

6. Порядок подключения рабочих станций к сетям общего пользования

6.1. Сеть общего пользования является открытой системой передачи данных, при работе в которой могут возникнуть следующие основные угрозы безопасности информации:

6.1.1. заражение информационно-вычислительных ресурсов программными вирусами;

6.1.2. внедрение в автоматизированные системы программных закладок;

6.1.3. загрузка трафика нежелательной корреспонденцией (спамом);

6.1.4. несанкционированная передача конфиденциальной информации, в т.ч. ПДн пользователями ИС в сети общего пользования.

6.2. Для предотвращения указанных угроз Администратору информационной безопасности необходимо:

6.2.1. разграничить доступ пользователей к ресурсам сетей общего пользования путём использования средств межсетевого экранирования защищённого сегмента локальной вычислительной сети, в котором происходит обработка конфиденциальной информации, в т.ч. ПДн;

6.2.2. осуществлять контроль за конфиденциальной информацией, в т.ч. ПДн, выходящими из ОИ Организации и загружаемых из сети общего пользования;

6.2.3. передача конфиденциальной информации, в т.ч. ПДн при использовании каналов связи сети общего пользования должна осуществляться только с применением средств криптографической защиты информации.

7. Порядок применения средств организации архивирования, резервирования и восстановления прикладного программного обеспечения и персональных данных

7.1. Администратор информационной безопасности осуществляет контроль за процессом архивирования, резервирования и восстановления прикладного программного обеспечения и персональных данных.

7.2. Средства организации архивирования и восстановления прикладного программного обеспечения должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в Организации.

7.3. Порядок применения средств организации архивирования и восстановления прикладного программного обеспечения устанавливается с учетом соблюдения следующих требований:

7.3.1. обязательное хранение всех архивов в защищенном месте;

7.3.2. частота архивации данных зависит от их важности и частоты их изменения;

7.3.3. системные папки операционной системы необходимо архивировать после серьезных изменений конфигурации;

7.3.4. данные, которые изменяются очень редко, не имеет смысла архивировать.

7.3.5. восстановление работоспособности программных средств и информационных массивов, в случае утери и повреждения.

7.4. Организации архивирования и восстановления прикладного программного обеспечения подлежат следующие файлы и документы:

7.4.1. все файлы операционной системы и установленных приложений. Архивирование системных файлов должно производиться только после установки новых приложений или обновления самой операционной системы;

7.4.2. личные профили пользователей;

7.4.3. папки, содержащие важные документы;

7.4.4. базы данных;

7.4.5. другие файлы и папки, представляющие ценность.

7.5. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

7.5.1. системы жизнеобеспечения;

7.5.2. системы обеспечения отказоустойчивости;

7.5.3. системы резервного копирования и хранения данных;

7.5.4. системы контроля физического доступа.

Системы жизнеобеспечения ИС включают:

7.5.5. пожарные сигнализации и системы пожаротушения;

7.5.6. системы вентиляции и кондиционирования;

7.5.7. системы резервного питания.

7.6. Все критичные помещения Организации (помещения, в которых размещаются элементы ИС и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

7.7. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИС в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

7.8. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

7.8.1. локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

7.8.2. источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

7.8.3. дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

7.8.4. резервные линии электропитания в пределах комплекса зданий;

7.8.5. аварийные электрогенераторы;

7.8.6. системы обеспечения отказоустойчивости (кластеризация; технология RAID).

7.9. Резервное копирование и хранение данных должно осуществлять на периодической основе:

7.9.1. для обрабатываемых персональных данных – не реже раза в неделю;

7.9.2. для технологической информации – не реже раза в месяц;

7.9.3. эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых

осуществляется их установка на элементы ИС – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

7.10. Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

7.11. Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

7.12. Носители должны храниться не менее года, для возможности восстановления данных.

8. Порядок реагирования на аварийную ситуацию

8.1. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИС, предоставляемых пользователям ИС.

8.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться Администратором информационной безопасности в «Журнале по учету мероприятий по контролю».

8.3. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование предпринимают меры по восстановлению нарушенной работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

8.4. При реагировании на инцидент, важно правильно классифицировать критичность инцидента. Критичность оценивается на основе следующей классификации:

8.4.1. Уровень 1 – Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИС и средств защиты.

8.4.2. Уровень 2 – Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИС и средств защиты.

8.4.3. Уровень 3 – Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИС и средств защиты, а также к угрозе жизни пользователей ИС, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к нарушению работоспособности ИС и средств защиты на сутки и более.

8.5. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций.

8.6. Все критичные помещения МУ «ДК «Матыра» (помещения, в которых размещаются элементы ИС и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

8.7. Администратором информационной безопасности должно быть проведено обучение должностных лиц, имеющих доступ к ресурсам ИС, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

8.7.1. оказание первой медицинской помощи;

8.7.2. пожаротушение;

8.7.3. эвакуация людей;

8.7.4. защита материальных и информационных ресурсов;

8.7.5. методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;

8.7.6. выключение оборудования, электричества, водоснабжения, газоснабжения.

8.8. Администратор информационной безопасности должен быть дополнительно обучен методам частичного и полного восстановления работоспособности элементов ИС.

8.9. Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

9.Действия в случае нештатных ситуаций

9.1. Администратором информационной безопасности предусматривается возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

9.2. Для обеспечения возможности восстановления программного обеспечения в информационной системе приняты соответствующие планы по действиям персонала (администраторов безопасности, пользователей) при возникновении нештатных ситуаций (Инструкция по действиям персонала в нештатных ситуациях).

9.3. Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций предусматривает:

9.3.1.восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;

9.3.2.восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;

9.3.2.возврат ИС в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей ИС, определенных администратором информационной безопасности, позволяющих решать задачи по обработке информации.

9.3.3. Администратором информационной безопасности применяются компенсирующие меры защиты информации в случаях, когда восстановление работоспособности системы защиты информации невозможно.

10. Организация обучения

10.1 Уровень знаний Администратора информационной безопасности должен быть достаточным для выполнения работ по настройке, поддержания в работоспособном состоянии и контроля эффективности системы защиты конфиденциальной информации, в том числе персональных данных.

10.2 Обучение Администратора информационной безопасности включает подготовку по следующим направлениям:

10.2.1 методы и способы противодействия несанкционированному доступу к защищаемой конфиденциальной информации;

10.2.2 методы и способы противодействия утечки информации по каналам побочных электромагнитных излучений и наводок;

10.2.3 методы и способы противодействия вирусным угрозам (использование антивирусного программного обеспечения);

10.2.4 методы и способы обнаружение сетевых вторжений в сегмент локальной вычислительной сети, в котором производится обработка конфиденциальной информации, в том числе персональных данных;

10.2.5 криптографические методы защиты конфиденциальной информации при ее передаче по открытым каналам связи;

10.2.6 основы законодательства Российской Федерации в области обеспечения безопасности информации.

10.3 В ходе выполнения своих должностных обязанностей Администратору информационной безопасности необходимо проводить периодический инструктаж пользователей средств вычислительной техники по правилам работы с используемыми средствами и системами защиты информации.

10.4 Инструктажи проводятся в помещениях МУ «ДК «Матыра», непосредственно на рабочих местах пользователей ПЭВМ, обрабатывающих конфиденциальную информацию.

10.5 В ходе инструктажей освещаются следующие вопросы:

10.5.1 правила работы со средствами защиты информации от несанкционированного доступа;

10.5.2 правила работы с персональными идентификаторами;

10.5.3 правила парольной защитой ПЭВМ;

10.5.4 правила работы с антивирусными средствами, в том числе при использовании отчуждаемых (сменных) носителей;

10.5.5 правила работы с криптографическими средствами защиты конфиденциальной информации при ее передаче по открытым каналам связи.

10.6 Помимо периодических инструктажей Администратор информационной безопасности проводит первичный инструктаж вновь допущенных к конфиденциальной информации сотрудников МУ «ДК «Матыра», по правилам работы с используемыми средствами и системами зашиты информации. Освещаемые вопросы в ходе первичного инструктажа аналогичны вопросам при периодических инструктажах.