Приложение № 5 к приказу
от 13.01 2017 г. № 3
УТВЕРЖДЕНО
Начальник МБОУ «МиРЦ»
от «13» 01 2017 г.

_____ Маяцкая И.Г.
(подпись)

Политика информационной безопасности Муниципального бюджетного образовательного учреждения «Методический и ресурсный центр»

1. Термины и определения

Безопасность информации ограниченного доступа – состояние защищенности информации ограниченного доступа, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах с информацией ограниченного доступа.
Доступ к информации – возможность получения информации и ее использования.
Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
Информация ограниченного доступа – любая информация, отнесенная к конфиденциальной информации, а именно: персональные данные, служебная тайна, врачебная тайна или иная информация, доступ к которой ограничен в соответствии с нормативно-правовыми актами Российской Федерации.
Информационная система с информацией ограниченного доступа – информационная система, представляющая собой совокупность информации ограниченного доступа, содержащихся в базе данных или в виде отдельных файлов с данными, а также информационных технологий и технических средств, позволяющих осуществлять обработку такой информации с использованием средств автоматизации или без использования таких средств.
Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.
Неправомерные действия с информацией ограниченного доступа – преднамеренное или случайное несанкционированное ознакомление с информацией ограниченного доступа, ее копирование, распространение, передача, уничтожение, изменение (модификация), блокирование, а также любое иное несанкционированное использование, которое может нанести ущерб Обществу или государству.
Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа.
Обработка информации ограниченного доступа – действия (операции) с информацией ограниченного доступа, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение.
Пароль – секретная (конфиденциальная) строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системы для получения доступа

к данным и программам; является средством защиты данных от несанкционированного доступа.

Пользователь – работник, использующий ресурсы информационной системы для выполнения должностных обязанностей.

Правила разграничения доступа– совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Распространение информации ограниченного доступа – действия, направленные на передачу такой информации определенному кругу лиц или на ознакомление с информацией ограниченного доступа неограниченного круга лиц, в том числе ее обнародование в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ней каким-либо иным способом.

Технические средства информационной системы–средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации ограниченного доступа (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

2. Общие положения

Необходимость разработки настоящей Политики информационной безопасности Муниципального бюджетного образовательного учреждения «Методический и ресурсный центр» (далее – Политики) обусловлена применением новейших информационных технологий и процессов при обработке информации вообще, и информации ограниченного доступа в частности.

Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский и Уголовный кодексы Российской Федерации, Федеральные конституционные законы Российской Федерации, федеральные законы Российской Федерации, Указы и распоряжения Президента Российской Федерации, постановления и распоряжения Правительства Российской Федерации, другие нормативные документы действующего законодательства Российской Федерации, документы Государственной технической комиссии при Президенте Российской Федерации, Федерального агентства правительственной связи и информации при Президенте Российской Федерации, Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Политика является основой для:

- формирования и проведения единого подхода в области обеспечения безопасности информации в Муниципальном бюджетном образовательном учреждении «Методический и ресурсный центр» (далее – Учреждение);
- принятия управленческих решений и разработки практических мер по воплощению Политики и выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз информационной безопасности;
- координации деятельности Учреждения при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению информационной безопасности;
- разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения информационной безопасности.

3. Цель

Основными целями данной Политики являются:
- установка правил размещения информации на официальных информационных ресурсах Учреждения;
- установка правил использования программного обеспечения в Учреждении;
- установка правил обеспечения сохранности имущества, а также правил его эксплуатации, необходимых для обеспечения информационной безопасности в Учреждении;
- установка правил создания, передачи и обеспечения сохранности паролей;
- установка правил предотвращения, обнаружения и устранения последствий компьютерных вирусов и вредоносных программ;
- установка правил использования межсетевых экранов, их развертывания, обеспечения безопасности и тестирования;
- установка правил получения доступа к сетям общего пользования, правил работы в них, ограничений по их использованию, обеспечению безопасности при работе с ними и действия при их нарушении;
- установка правил использования электронной почты;
- установка правил резервного копирования информации в электронном виде;
- установка правил использования беспроводных сетей;
- установка правил использования средств криптографической защиты информации, обеспечение выполнения требований нормативно-правовых актов Российской Федерации по порядку использования средств криптографической защиты информации;
- установка правил использования мобильных устройств, обеспечения их безопасности и сохранности;
- установка правил использования отчуждаемых устройств, обеспечения их безопасности и сохранности;
- установка правил работы в локальных вычислительных сетях, направленных на повышения безопасности их эксплуатации;
- установка правил доступа к информационным ресурсам, направленных на повышение информационной безопасности;
- совершенствование работы с кадровым составом (работниками) Учреждения, направленное на повышение безопасности информации;
- выработка подходов к организации постоянного повышения осведомленности с кадрового состава (работников) Учреждения, направленное на повышение безопасности информации;
- выработка подходов к организации взаимодействия с третьими лицами, направленных на повышение безопасности информации;
- осуществление деятельности по обеспечению информационной безопасности в соответствии с требованиями нормативно-правовых актов Российской Федерации.

4. Область применения

Областью применения являются работники Учреждения, а также лица, состоящие в договорных отношениях с Учреждением, подразумевающих исполнение требований настоящей Политики и имеющие доступ к информационным ресурсам Учреждения.

5. Меры обеспечения информационной безопасности

5.1. Размещение информации на официальных информационных ресурсах

Официальные материалы, подлежащие размещению на официальных информационных ресурсах Учреждения. Дополнительно допускается размещение в прочих официальных информационных ресурсах.

Содержание официальных материалов должно удовлетворять требованиям нормативно-правовых актов Российской Федерации. Ответственность за соответствие содержания официальных материалов требованиям нормативно-правовых актов Российской Федерации возлагается на работника, уполномоченного и согласовавшего размещение таковых материалов.

Размещение официальных материалов на официальных интернет-порталах осуществляется Учреждением самостоятельно, за исключением случаев, предусмотренных прочими нормативными документами.
Содержание официальных материалов должно быть общедоступно и содержать свободно распространяемую информацию.
Размещение в официальных материалах информации (материалов) из сторонних источников (авторов) должно осуществляться с соблюдением требований нормативно-правовых актов Российской Федерации в сфере защиты авторских прав и интеллектуальной собственности.
В соответствии с нормативными правовыми актами Российской Федерации публикация в официальных материалах информации ограниченного доступа и составляющих государственную тайну запрещена.
Обладателем информации, публикуемой на официальных интернет-порталах, является Учреждение, предоставляющее данные материалы.

5.2. Использование программного обеспечения

Программное обеспечение, используемое для осуществления деятельности Учреждения, должно соответствовать условиям его лицензирования (независимо от того, является ли оно коммерческим или свободно распространяемым) и использоваться строго в соответствии с лицензионным соглашением. Случаи хранения и/или использования программного обеспечения, не являющегося лицензионным, должны быть исключены.
В случае, если нормативно-правовыми актами Российской Федерации предъявляются особые требования к программному обеспечению (например, требование по сертификации такого программного обеспечения уполномоченными организациям и т.п.) необходимо обеспечить выполнение подобных требований.
На каждое автоматизированное рабочее место должен быть установлен комплект программного обеспечения, необходимый и достаточный для выполнения на нем поставленных задач.
Учреждение предоставляет работникам достаточное количество лицензий на использование программного обеспечения, необходимого для выполнения работником своих должностных обязанностей.

5.3. Обеспечение физической безопасности

Все серверные помещения Учреждения должны отвечать требованиям нормативно-правовых актов Российской Федерации в части оборудования устройствами сигнализации (например, пожарной, охранной и т.п.).
Помещения, которые должны быть оборудованы дополнительными устройствами регистрации, контроля и поддержания заданных характеристик (например, система автоматического пожаротушения, контроля влажности, принудительной вентиляции, кондиционирования воздуха, защиты от статического электричества и т.п.), в соответствии с нормативно-правовыми актами Российской Федерации или правилами эксплуатации оборудования, размещенного в таких помещениях, и требуемых для соблюдения гарантийных обязательств производителя, должны быть полностью укомплектованы подобными устройствами.

5.3.1. Организация охраны

В помещениях, в которых размещается имущество Учреждения, должна иметься возможность организации круглосуточной охраны. В помещениях, расположенных в зданиях, в которых возможно использование услуг служб централизованной охраны здания, охрана должна осуществляться силами таких служб. В помещениях, расположенных в зданиях без служб централизованной охраны, охрана должна осуществляться за счет привлечения специализированных организаций, предоставляющих услуги по круглосуточной охране.

5.3.2. Контроль доступа

Все помещения Учреждения должны быть оборудованы дверьми, закрываемыми на замок.

Должен быть предусмотрен механизм установления личности осуществляющей санкционированное вскрытие помещений (например, проверка удостоверения личности, применение систем контроля и управления доступом, роспись за получения ключа от помещений на посту охраны и т.п.).
Отдельные группы помещений, нахождение в которых посторонних лиц не требуется (например, серверные и архивные помещения), могут отделяться дополнительными дверьми, иными средствами ограничения доступа.
Помещения, доступ в которые согласно нормативно-правовым актам Российской Федерации должен быть ограничен, а также в которых хранится или обрабатывается информация ограниченного доступа, хранятся товарно-материальные ценности и иные подобные помещения, должны быть оборудованы механизмом ограничения доступа (автоматизированная система контроля доступа, устройства для опечатывания и т.п). Работники, имеющие право самостоятельного вскрытия таких помещений должны быть определены приказом, утверждаемым директором Учреждения. Двери в такие помещения должны быть оборудованы механизмом автоматического их закрытия.
Работники не должны оставлять свои рабочие кабинеты без наблюдения. В случае если помещение остается без наблюдения, помещение должно быть закрыто на замок.

5.3.3. Контроль нахождения посторонних лиц в помещениях

Проход посетителей или представителей сторонних организаций в здание и контроль их нахождения в помещениях, должен осуществляться в соответствии с организационно-распорядительными документами Учреждения по порядку обеспечения пропускного режима в задание.
Работники сторонних организаций (например, обслуживающий персонал здания, работники, осуществляющие сопровождение программного обеспечения, работник осуществляющие ремонт оборудования и т.п.) должны вызываться установленным порядком в случае такой необходимости. При приходе таких работников без предварительной заявки их допуск в помещения должен осуществляться только по согласованию с уполномоченным лицом Учреждения, в ведении которого предполагаются проводимые работы.

5.3.4. Эксплуатация электронных устройств

5.3.4.1. Безопасность эксплуатации

В соответствии с нормативными правовыми актами Российской Федерации размещение экранов автоматизированных рабочих мест, обрабатывающих информацию ограниченного доступа, должно исключать возможность их просмотра лицами, не допущенными к данной информации.
При использовании систем видеонаблюдения, такие системы должны быть установлены в местах, исключающих просмотр содержимого экранов автоматизированных рабочих мест, обрабатывающих информацию ограниченного доступа, а также исключающих просмотр вводимых паролей, кодов и т.п.
Системные блоки автоматизированных рабочих мест, периферийное оборудование, используемое для обработки информации ограниченного доступа, должно быть опечатано или оборудовано иным способом ограничения их несанкционированного вскрытия.

5.3.4.2. Ограничения при эксплуатации

Работникам запрещено подключать собственные технические средства, периферийные устройства, за исключением учтенных в Учреждении носителей информации, к автоматизированным рабочим местам и сети Учреждения без письменного согласования ответственного за информационную безопасность.
Запрещено устанавливать собственные комплектующие в технические средства, находящиеся на балансе Учреждения.

5.3.4.3. Профилактическое обслуживание и иные правила эксплуатации

Все технические средства должны проходить техническое обслуживание. Такое обслуживание должно проводиться регулярно, но не реже сроков, указанных в

эксплуатационной документации или организационно-распорядительных документах Учреждения.
Проведение технического обслуживания должно обеспечиваться работниками отдела системного программного обеспечения и сетевых технологий Учреждения, при обязательном согласовании с отделом по защите информации или производиться с привлечением квалифицированных специалистов сторонних организаций, имеющих необходимый перечень лицензий на осуществление отдельных видов деятельности, в соответствии с нормативными правовыми актами Российской Федерации.
Технические устройства, необходимые для выполнения работниками своих должностных обязанностей рекомендуется оборудовать сетевыми фильтрами.
Сетевые, питающие и иные кабеля должны быть проложены в соответствии с отраслевыми стандартами. Соблюдение отраслевых стандартов должно исключить повреждение таких кабелей при повседневной работе, а также минимизировать вероятность получения травм, вызванных нарушениями укладки таких кабелей.

5.3.4.4. Прекращение эксплуатации

Перед передачей (в том числе для ремонта) сторонним организациям, списанием или прекращением использования оборудования, участвовавшего в обработке информации ограниченного доступа, уполномоченными лицами должна быть проведена проверка, с целью исключения попадания такой информации третьим лицам.

5.4. Обеспечение антивирусной защиты

Антивирусное программное обеспечение должно быть установлено и функционировать в штатном режиме на всех межсетевых экранах (в программном исполнении), FTP-серверах, почтовых и прочих серверах Учреждения, автоматизированных рабочих местах отдельно стоящих и подключенных к локальным вычислительным сетям (в том числе к корпоративной сети Учреждения) и портативных компьютерах.
Не допускается такое изменение настроек системы антивирусной защиты, в части оповещения о нахождении компьютерных вирусов или вредоносных программ, в результате которого уменьшается эффективность данной системы.
Обновление баз системы антивирусной защиты должно производиться регулярно. Построение системы антивирусной защиты должно предусматривать возможность обновления ее антивирусных баз и компонентов производителем по мере их создания. В случае невозможности такого построения системы (например, отдельно стоящие автоматизированные рабочие места в удаленных подразделениях не подключенные к каким-либо сетям), обновление системы антивирусной защиты должно производиться с регулярностью, обеспечивающей ее эффективное функционирование.
Запрещается отключение системы антивирусной защиты, за исключением случаев проведения тестирования программного обеспечения и иных тестов, проводимых уполномоченными работниками Учреждения.

5.4.1. Предотвращение выполнения вредоносного кода

Учреждение обязано производить сканирование своих информационных ресурсов, а также всех автоматизированных рабочих мест на наличие компьютерных вирусов и/или вредоносных программ.
Файлы, полученные любым образом, с любых носителей информации или сетей общего пользования должны быть проверены на наличие вредоносного кода.
Подключение к автоматизированным рабочим местам незарегистрированных отчуждаемых носителей информации (дискеты, компакт-диски, съемные жесткие диски, сотовые телефоны, карманные персональные компьютеры, фотоаппараты и иные носители информации) разрешено с обязательной проверкой «по требованию» таких носителей информации на наличие компьютерных вирусов и/или вредоносных программ после согласования с отделом по защите информации.
В случае получения файлов, проверка которых в исходном состоянии невозможна (например, файлы содержат архивы, не поддерживаемые системой антивирусной защиты,

файлы прошли криптографическое преобразование и т.п.), необходимо, привести данные файлы к состоянию пригодному для проверки на наличие вредоносного кода (на автоматизированном рабочем месте, не подключенном к локальным вычислительным сетям Учреждения), осуществить такую проверку, после чего принимать решение о возможности использования данных файлов.

Пользователи, которые в соответствии с должностными обязанностями используют портативные компьютеры, должны в обязательном порядке соблюдать требования настоящей Политики в их отношении.

Все файлы, передаваемые третьим лицам, должны быть проверены на наличие вредоносного кода системой антивирусной защиты до их передачи.

Любые намеренные попытки написания, компиляции, хранения, запуска, пропагандирования или распространения пользователями компьютерных вирусов или вредоносных программ, а также иного кода предназначенного для саморазмножения, нанесения ущерба или снижения производительности систем Учреждения, запрещены.

5.4.2. Обнаружение вредоносного кода

В случае обнаружения системой антивирусной защиты компьютерного вируса или вредоносной программы пользователь обязан выключить компьютер и сообщить об этом уполномоченному работнику Учреждения.

О любом инциденте, связанном с выявлением компьютерного вируса или вредоносных программ, на автоматизированном рабочем месте или портативном компьютере, подключаемом к сети Учреждения, должно быть сообщено в отдел по защите информации.

Самостоятельные попытки пользователя по удалению компьютерного вируса или вредоносной программы запрещены.

В случае обнаружения в сети Учреждения компьютерных вирусов или вредоносных программ в сообщениях электронной почты, систем мгновенного обмена сообщениями и т.п., данные сообщения будут удалены.

Файлы, содержащие вредоносный код, должны быть удалены системой антивирусной защиты.

5.5. Межсетевое экранирование

Для обеспечения информационной безопасности при присоединении к локальным вычислительным сетям сторонних организаций, такие присоединения должны быть защищены межсетевыми экранами, не зависимо от используемых технологий подключения (например, подключение с использование беспроводных сетей, модемов и т.п.), отвечающих требованиям нормативно-правовых актов Российской Федерации.

Компьютеры, обрабатывающие информацию ограниченного доступа, должны быть отделены от остальной части сети межсетевыми экранами, отвечающими требованиям нормативно-правовых актов Российской Федерации, в соответствии с типом такой информации. Допускается как группировка автоматизированных рабочих мест по типу обрабатываемой информации и отделение всей группы одним межсетевым экраном, так и установка персональных межсетевых экранов на каждое автоматизированное рабочее место.

5.5.1. Требования по размещению межсетевых экранов

Межсетевые экраны, отделяющие большие группы автоматизированных рабочих мест, включая межсетевые экраны, отделяющие внутреннюю часть локальных вычислительных сеть от сетей общего пользования, должны быть установлены в помещениях с контролируемым доступом (в случае программного исполнения межсетевых экранов, они должны устанавливаться на автоматизированных рабочих местах, расположенных в помещениях с контролируемым доступом).

Межсетевые экраны, отделяющие большие группы автоматизированных рабочих мест, включая межсетевые экраны отделяющие внутреннюю сеть от сетей общего пользования, должны быть, установлены на специализированных аппаратных платформах или на

выделенных (физических или виртуальных) автоматизированных рабочих местах, не выполняющих дополнительные функции. На автоматизированных рабочих местах с развернутыми межсетевыми экранами, отделяющих внутреннюю сеть от сетей общего пользования и/или большую группу автоматизированных рабочих мест, разрешено хранение только информации, необходимой для выполнения межсетевым экраном своих функций. На таких автоматизированных рабочих местах должен быть установлен минимальный набор программного обеспечения, необходимый для выполнения межсетевым экраном своих функций.

5.5.2. Требования по развертыванию межсетевых экранов

Перед развертыванием межсетевого экрана, отделом по защите информации Учреждения должна быть составлена диаграмма разрешенных маршрутов, с описанием протоколов, разрешенных к применению на данных маршрутах. Разрешение на использование маршрутов и протоколов предоставляется только в случае их необходимости для выполнения Учреждением его функций и задач, выполнения должностных обязанностей его работниками, и в случае достаточности принятых мер для обеспечения безопасности их использования. Соответствие настроек межсетевых экранов данным диаграммам должно проверятся уполномоченными лицами (работниками отдела по защите информации) регулярно, но не реже 2 раз в год.

При однотипности настройки нескольких межсетевых экранов допускается использование описания групповых политик (например, настройка межсетевых экранов бухгалтерии, настройка персональных межсетевых экранов руководителей структурных подразделений Учреждения и т.п.).

Использование всех маршрутов и протоколов, которое отдельно не разрешено данной Политикой или сопутствующими документами, разработанными отделом по защите информации Учреждения должно блокироваться устройствами межсетевого экранирования. Перечень разрешенных, на текущий момент времени, маршрутов и протоколов должен находиться у уполномоченного работника (в отделе по защите информации Учреждения).

5.5.3. Требования по обеспечению безопасности межсетевых экранов

Все межсетевые экраны должны иметь уникальные пароли и/или другие дополнительные механизмы контроля доступа. В случаях, когда производителем межсетевого экрана поддерживается механизм усиленной аутентификации, данный механизм должен быть задействован. Доступ к механизмам настройки систем межсетевого экранирования должен осуществляться либо непосредственно с автоматизированного рабочего места, на котором развернут межсетевой экран, либо удаленно (в случае удаленного доступа через сети общего пользования необходимо использование криптографического преобразования передаваемой информации).

Доступ к информации о внутренней адресации, конфигурации сети, используемом программном обеспечении и любая подобная информация о структуре сети, из сетей общего пользования должен быть максимально ограничен.

Программное обеспечение межсетевых экранов должно быть обновлено до последней версии, в рамках имеющихся лицензионных соглашений. В случае поддержки программным обеспечением межсетевых экранов механизма автоматического обновления, такой механизм должен использоваться. В ином случае все обновления должны устанавливаться в течение двух рабочих дней после их предоставления производителем.

5.5.4. Использование демилитаризованных зон

Сервера Учреждения, предназначенные для доступа из сетей общего пользования, должны быть вынесены в демилитаризованную зону, подсеть защищенную от доступа как из сетей общего пользования, так и из внутренних локальных вычислительных сетей Учреждения одним или несколькими межсетевыми экранами.

Любое прямое подключение к ресурсам демилитаризованной зоны, не проходящее через межсетевой экран, запрещено.

5.5.5. Восстановление межсетевых экранов

Актуальная резервная копия конфигурационных файлов межсетевых экранов, используемые правила, документы, регламентирующих эксплуатацию и настройку межсетевых экранов должны находиться в доступности системных администраторов и администраторов информационной безопасности Учреждения, но исключать возможность получения доступа со стороны третьих лиц. В случае поддержкой производителем автоматического резервного копирования конфигурационных файлов и восстановление из резервных копий при несанкционированном их изменении, данные механизмы должны быть задействованы.

5.5.6. Тестирование межсетевых экранов

Тестирование межсетевых экранов должно производиться регулярно, но не реже двух раз в год. Процесс тестирования должен включать проверку соответствия параметров настройки межсетевого экрана согласованным требованиям к его настройке и реальной ситуации, перечня разрешенных протоколов, перечня разрешенных маршрутов, анализ журнала регистрации событий, установки последних обновлений. При проведении тестирования допускается проведение «тестов на проникновение», которое, в то же время, не является обязательным. Проведение «теста на проникновение» должно осуществляться только с привлечением сторонних организаций, имеющих соответствующих специалистов. При проведении «теста на проникновение» правила его проведения и соглашение о конфиденциальности с его участниками должны быть согласованы с отделом по защите информации Учреждения и подписаны официальными представителями участников.

Для проведения различного рода анализов, программное обеспечение межсетевых экранов должно быть настроено на автоматическое сохранение следующих событий (ведение log-файлов):

- внесение изменений в параметры настройки межсетевого экрана;
- изменение разрешенных протоколов;
- изменение разрешенных маршрутов;
- несанкционированный доступ или попытки несанкционированного доступа к настройкам межсетевых экранов;
- обход используемых механизмов защиты или его попытки.

При наличии возможности log-файлы должны быть защищены от несанкционированного изменения с применением электронной подписи, криптографического преобразования или иных схожих мер. Log-файлы должны регулярно, но не реже одного раза в месяц, подвергаться резервному копированию. Срок хранения log-файлов должен составлять не менее шести месяцев. Содержимое log-файлов должно регулярно, но не реже двух раз в год, анализироваться для подтверждения правильности функционирования межсетевого экрана.

5.6. Использования сетей общего пользования

Вся информация, полученная из сетей общего пользования, должна считаться недостоверной, не будучи подтвержденной из других источников. Перед использованием свободно распространяемой информации из сетей общего пользования для принятия решений в рамках деятельности Учреждения, такая информация должна быть перепроверена в других источниках.

Учреждение не несет ответственности за информацию, содержащуюся в сетях общего пользования. В случае открытия пользователем ресурсов, содержание которых может считаться незаконным или оскорбительным, например, материалы сексуального характера, расистские, дискредитирующие, оскорбительные, непристойные, уничижительные, дискриминационные, угрожающие, пользователь обязан прекратить работу с данным ресурсом.

5.6.1. Обеспечение безопасности использования сетей общего пользования

Для получения возможности доступа пользователя в сети общего пользования (далее – СОП) необходимо использование технологий идентификации и аутентификации, а также должны быть обеспечены механизмы защиты информационных ресурсов Учреждения от воздействия из сетей общего пользования.

Пользователям запрещено использование любых способов доступа в сети общего пользования (например, dial-up доступ, использование для соединения с СОП операторов сотовой связи и т.п.) отличных от установленных. В случаях, если необходимо осуществлять доступ в сети общего пользования, отличный от установленных (для работы с банковскими системами и т.п.), то такой доступ должен быть согласован с уполномоченным работником Учреждения.

Передача информации ограниченного доступа по сетям общего пользования, допускается при условии соблюдения всех требований, определяемых нормативными правовыми актами Российской Федерации, к такой передаче.

Пользователю запрещено любое тестирование и/или попытки обхода установленных механизмов защиты.

5.6.2. Ограничение предоставления доступа к СОП

Запрещено предоставлять доступ в сети общего пользования стороннему обслуживающему персоналу и иным лицам, состоящим в договорных отношениях с Учреждением, за исключением случаев, когда такой доступ необходим для решения данными лицами задач в их интересах. Доступ может быть предоставлен только по согласованию с отделом по защите информации Учреждения.

Получение доступа пользователя к ресурсам сети общего пользования, не означает, что пользователь имеет неограниченные возможности при работе с данным ресурсом. Уполномоченными работниками Учреждения могут приниматься меры по предотвращению отдельных действий пользователя при работе с ресурсами сетей общего пользования, как-то ограничение по загрузке отдельных файлов, отображение объявлений рекламного, порнографического и иного характера и т.п.

5.6.3. Ограничения использования сетей общего пользования

Использование СОП для личных нужд пользователя запрещен. Доступ пользователей предоставляется к определенным информационным ресурсам СОП, необходимость использования которых обусловлена выполнением должностных обязанностей. В отдельных случаях, пользователям может быть предоставлен неограниченный доступ к ресурсам СОП. Доступ предоставляется по письменной заявке, согласованной уполномоченным работником отдела по защите информации Учреждения. Использование ресурсов Учреждения для участия в игровых, развлекательных и иных ресурсах (включая конкурсы, выставки, социальные сети и иные Интернет-сообщества) запрещено. В отдельных случаях, по указанию директора Учреждения, пользователям могут предоставляться дополнительные права для работы с такими ресурсами.

Пользователь обязан понимать, что при работе в СОП передаваемые данные, не прошедшие криптографическое преобразование, доступны для просмотра третьими лицами. Передача информации ограниченного доступа без соблюдения требований, предъявляемых к ее передаче по СОП, запрещена.

Пользователям запрещена загрузка любого программного обеспечения из СОП. В исключительных случаях, когда загрузка такого программного обеспечения продиктована выполнением Учреждением его функций и задач, загрузка программного обеспечения из сетей общего пользования осуществляется уполномоченными работниками после согласования с отделом системного программного обеспечения и сетевых технологий, а также с отделом по защите информации Учреждения.

Пользователям запрещено участвовать в обмене пиратским программным обеспечением, серийными номерами программного обеспечения, номерами украденных кредитных карт

и ином обмене, нарушающем и/или ущемляющем права правообладателей обмениваемой информации.

5.6.4. Правила использования сетей общего пользования

Искажение, маскировка или замена идентификационной информации пользователя в СОП или в любых системах электронного обмена информации запрещена. Имя пользователя, адреса корпоративной электронной почты, служебное и иная сопутствующая информация, указываемая в сообщениях или размещаемая в сетях общего пользования, должна отражать достоверную информацию об авторе сообщения или размещаемой информации. Использование пользователем любого программного обеспечения, технических средств и технологий, предполагающих анонимность действий пользователей, запрещено.

Пользователям запрещено размещать любую информацию о деятельности Учреждения в СОП, кроме информации, размещаемой в соответствии с требования нормативно-методическими документами Российской Федерации.

В любых сообщениях и публикациях в СОП, в которых есть ссылка на аффилированность пользователя с Учреждением, не допускается использование агрессивных высказываний. Пользователю запрещено угрожать как отдельным личностям, так и организациям. Сообщения и публикации с информацией раздражающей, надоедающей и беспокоящей других лиц запрещено.

Для облегчения обмена данными между пользователями локальной сети, системным администратором создана папка обмена доступная пользователям локальной сети. Процедура обмена данными проста, но тем не менее подчинена правилам политики информационной безопасности. Время хранения файла в папке обмена составляет не более 5 минут. Папка обмена создана для обмена данными а не для хранения данных! Запрещено сохранять данные в папке обмена более регламентированного времени!

5.6.5. Анализ использования пользователем сетей общего пользования

В целях выявления нецелевого использования ресурсов, Учреждение может собирать информацию о посещенных пользователем ресурсах сетей общего пользования, загруженных файлах, времени проведенном на отдельных ресурсах сетей общего пользования и иной связанной информации. Данная информация может быть использована для анализа использования пользователем сетей общего пользования в соответствии с предоставленными ему полномочиями, в рамках выполнения пользователем своих должностных обязанностей.

В любое время, без предварительного предупреждения, отдел по защите информации Учреждения в праве провести анализ передаваемых электронных сообщений, содержимого log-файлов, файлов, размещенных на автоматизированном рабочем месте пользователя, их настройку и конфигурацию, установленного на них программного обеспечения, а также любой другой информации находящейся на автоматизированном рабочем месте пользователя или передаваемой по локальным вычислительным сетям Учреждения или за ее пределы.

5.6.6. Сообщение о проблемах безопасности при работе с СОП

В случае перехвата информации или подозрения на него, пользователь обязан сообщить в отдел по защите информации Учреждения. В случае нарушений правил работы с СОП или подозрений на подобные нарушения работник обязан сообщить уполномоченному работнику отдела по защите информации Учреждения. В случае утраты, хищения или компрометации паролей или иной идентификационной информации или подозрении на данные события работник обязан уведомить отдел по защите информации Учреждения

В случае получения сообщения о выявленной уязвимости, пользователь обязан передать данное сообщение в отдел по защите информации Учреждения. Пользователю запрещено предпринимать любые самостоятельные попытки устранения уязвимостей, кроме указаний администраторов информационной безопасности. Пользователю запрещено самостоятельно передавать информацию о выявленных или потенциальных уязвимостях другим пользователям.

5.7. Использование электронной почты

5.7.1. Правила использования системы электронной почты

Все системы электронной почты должны быть использованы пользователями только для выполнения должностных обязанностей, выполнения договорных обязательств и выполнения требований нормативных правовых актов Российской Федерации.

Запрещено использовать электронную почту для отправления писем следующего содержания:

- писем, содержание которых может считаться незаконным или оскорбительным, например, материалы сексуального характера, расистские, дискредитирующие, оскорбительные, непристойные, уничижительные, дискриминационные, угрожающие, или иные подобные сообщения;
- любых подрывных, оскорбительных, неэтичных, незаконных или иначе недопустимых материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возрасте, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений или о национальном происхождении, гиперссылок или других ссылок на неприличные или очевидно оскорбительные веб-сайты и подобные материалы, шутки, массовые рассылки, предупреждений о вирусах и розыгрышей, обращений о помощи или вредоносного кода;
- писем, написанных таким образом, который может быть интерпретирован как официальная позиция или высказывание Учреждения, если это не разрешено в соответствии с нормативно-методическими документами Ростовской области.

Запрещено использовать корпоративную электронную почту в следующих целях:

- отправки сообщения с чужого почтового ящика или от чужого имени;
- отправки сообщений в личных или благотворительных целях, не связанных с задачами Учреждения;
- отправки большого объема данных (более 15 Мбайт);
- массовой рассылки писем, кроме случаев когда необходимо оповещение большого числа работников Учреждения или в случаях когда это обусловлено выполнением функций и задач Учреждения;
- в любых других незаконных, неэтичных и неразрешенных целях.

Работники, получившие электронную почту от другого пользователя, с сообщениями, содержащими запрещенное содержание обязаны уведомить о таком факте уполномоченного работника Учреждения.

Для отправки и/или получения сообщений, в рамках выполнения должностных обязанностей и/или относящихся к работе Учреждения, пользователям разрешено использовать только адреса корпоративной электронной почты.

В исключительных случаях, пользователь может принять решение об использовании системы электронной почты, отличной от корпоративной. При этом должны выполняться остальные положения настоящей Политики и требования нормативно-правовых актов Российской Федерации, Ростовской области и организационно-распорядительные документы Учреждения.

5.7.2. Безопасность при использовании системы электронной почты

Использование всех систем электронной почты должно осуществляться с применением технологий идентификации и аутентификации пользователя.

Отправка электронной почты, содержащей информацию ограниченного доступа, должна осуществляться в соответствии с требованиями, предъявляемыми к такой информации.

Пользователям запрещено открывать вложения в электронные сообщения, в случае если отправитель данного сообщения не известен пользователю. Открывать вложения от неизвестных отправителей допускается только администраторам.

Пользователям запрещено отвечать на запросы любой персональной идентификационной информации, включая пароли, коды доступа, номера кредитных карт и т.п. В случае

получения сообщений с такими запросами пользователь обязан сообщить о них в отдел защиты информации Учреждения.
Пользователям запрещено публиковать свои адреса корпоративной электронной почты в сетях общего пользования и открытых источниках информации. В случае возникновения такой необходимости для выполнения Учреждением его функций и задач, публикация адреса корпоративной электронной почты возможна в соответствии с нормативно-методическими актами Сахалинской области.
Массовые рассылки, не относящиеся к деятельности Учреждения, приходящие на адреса корпоративной электронной почты будут удалены.
Пользователи должны сообщать в отдел по защите информации о любых сообщениях, содержащих информацию о нарушении безопасности, выявленных уязвимостях и прочих предупреждениях.

5.7.3. Хранение сообщений системы электронной почты

Пользователь обязан регулярно проводить анализ сообщений, удаляя те из них, удаление которых не влияет на нормальную работу Учреждения и выполнение должностных обязанностей их работниками
В случае необходимости резервного копирования сообщений корпоративной электронной почты пользователь обязан направить заявку в отдел системного программного обеспечения и сетевых технологий Учреждения.

5.7.4. Стиль сообщений системы электронной почты

При ведении переписки с использованием системы электронной почты пользователи обязаны использовать деловой стиль общения, избегать фамильярности в обращении, использовать жаргонизмы и сознательно нарушать правила орфографии и пунктуации.

5.8. Резервное копирование

Резервное копирование информации, размещенной на автоматизированных рабочих местах пользователей сети Учреждения, может осуществляться Учреждением при наличии технической возможности.
Учреждение не несет ответственности за нарушение целостности и доступности рабочей информации в электронном виде, хранящейся на автоматизированных рабочих местах пользователя, если иное не определено нормативно-правовыми актами Российской Федерации.

5.8.1. Порядок резервного копирования рабочей информации

Политика распространяется только на информацию, необходимую для выполнения Учреждением его функций и задач и хранящуюся на определенных серверах.
Резервное копирование электронной переписки не осуществляется.
Резервное копирование должно сочетать как минимум две технологии резервного копирования, одной из которых должна быть технология RAID, обеспечивающая повышенную надежность хранимой информации, используемая для создания дисковых массивов в серверах.
Регулярность создания резервных копий рабочей информации должна быть достаточной для продолжения выполнения Учреждением их функций и задач, в случае нарушения целостности и/или доступности рабочей информации на выделенных серверах, но не реже одного раза в день для ежедневно изменяющихся данных и одного раза в неделю для периодически изменяющихся данных. Копирования резервных копий на отчуждаемые носители (внешние дисковые хранилища, ленточные накопители и т.п.) должно осуществляться регулярно, но реже одного раза в месяц.
Все рабочая информация, хранящаяся на выделенных серверах и регулярно копируемая на отчуждаемые носители, должна быть доступна для дальнейшего восстановления.
Как минимум одна резервная копия рабочей информации должна храниться на отчуждаемом носителе.
Процессы резервного копирования и восстановления для каждого отдельного типа информации должны быть документированы и периодически пересматриваться.

5.8.2. Порядок хранения резервных копий

Для хранения резервных копий на отчуждаемых носителях должны выбираться такие отчуждаемые носители, характеристики которых незначительно изменяются в течение предполагаемого времени хранения резервных копий.

Хранение резервных копий рабочей информации на отчуждаемых носителях должно осуществятся с организацией контролируемого доступа к данным носителям, их защитой от воздействия окружающей среды и не в одном помещении с серверами Учреждения, с которых осуществляется резервное копирование.

Условия хранения резервных копий информации ограниченного доступа должны отвечать требованиям нормативно-правовых документов Российской Федерации.

Срок хранения резервных копий на внешних носителях должен составлять не менее одного года, если иное не определено нормативно-правовыми актами Российской Федерации или внутренними организационно-распорядительными документами Учреждения.

Резервные копии, хранящиеся более одного года, должны ежегодно тестироваться, для подтверждения возможности их восстановления и использования.

5.9. Использование беспроводных сетей

Использование беспроводных сетей для создания локальных вычислительных сетей или их частей в Учреждении запрещено.

Пользователям запрещено развертывание собственных беспроводных сетей на территории Учреждения.

5.10. Использование средств криптографической защиты информации

Использование СКЗИ должно быть обусловлено требованиями нормативно-методических документов Российской Федерации и/или в соответствии с моделью нарушителя.

Деятельность с СКЗИ должна исключать нарушение законодательства Российской Федерации в области лицензирования. В случае, если предполагаемая деятельность с СКЗИ подразумевает необходимость получения лицензии, Учреждение обязано получить такую лицензию или привлекать для подобной деятельности сторонние организации, имеющие соответствующие лицензии.

При использовании СКЗИ для защиты информации ограниченного доступа данные криптографические средства должны соответствовать требованиям нормативно-правовым актам Российской Федерации, в том числе к их классу и сертификации.

Установка, настройка и техническое сопровождение СКЗИ должно осуществляться специалистами, прошедшими соответствующее обучение и не нарушать требования нормативно-правовых актов Российской Федерации.

Использование, в том числе хранение, СКЗИ должно отвечать требованиям законодательства Российской Федерации.

Перед использованием СКЗИ работники обязаны пройти обучение по порядку их использования.

Пользователям запрещено использование СКЗИ других пользователей, в том числе с целью выдать себя другого пользователя.

5.10.1. Управление ключами

Генерация и управление ключами не должно нарушать требований нормативно-правовых актов Российской Федерации.

В качестве устройств хранения закрытого ключа электронной подписи (далее – ЭП) разрешено использование только аппаратных устройств (различные виды token, смарт-карты и т.п.). Использование дискет для хранения закрытых ключей электронной подписи допускается, в крайнем случае, если иные аппаратные устройства не поддерживаются данной системой ЭП.

Обмен сообщениями, подписанными ЭП, возможен только при действующем сертификате открытого ключа электронной подписи.

Срок действия ЭП не должен превышать одного года и трех месяцев.

Пользователям запрещено передавать закрытые ключи ЭП, сертификат открытого ключа ЭП третьим лицам, за исключением случаев принадлежности ЭПУчреждению, как юридическому лицу. В таком случае использование ЭП возможно группой лиц, определенных директором Учреждения. Учреждение должно обеспечить работникам необходимые условия для хранения носителей с ключевой информацией, исключающих их.

Пользователям запрещено осуществлять резервное копирование ключевой информации (в том числе закрытых ключей ЭП) или делать копии сертификатов открытых ключей ЭП.

5.10.2. Использование электронной подписи

Для осуществления отдельных операций в своей деятельности Учреждением допускается использование ЭП, выданных различными удостоверяющими центрами (ЭП налоговой службы, пенсионного фонда, банков и т.п.).

Основанием для выдачи ЭПработнику Учреждения, для использования в информационных системах, является его заявление, утвержденное директором и содержащее реквизиты, необходимые для выдачи ЭП, в соответствии с требованиями удостоверяющего центра.

Ответственность за предоставление верных реквизитов и обеспечение соответствия порядка работы с электронной подписью требованиям нормативно-правовых актов Российской Федерации и удостоверяющего центра несет Учреждение и владелец ЭП в рамках своих полномочий.

Отправление сообщений, подписанных ЭП, разрешено только с адреса, указанного в сертификате владельца ЭП.

Передача ключей ЭП и сертификатов ЭП сторонним организациям может осуществляться с соблюдением требований нормативных правовых актов Российской Федерации.

5.10.3. Использование средств криптографической защиты для построения виртуальных частных сетей

При необходимости использования средств криптографической защиты для построения виртуальных частных сетей, отдел по защите информации определяет конкретный продукт, исходя из принципа совместимости с уже использующимися СКЗИ, если иное не определено в обосновании их использования.

Технические средства, отвечающие за управление СКЗИ и/или распределение ключевой информации, должны отвечать требованиям по информационной безопасности, определенным нормативно-правовыми актами Российской Федерации и документами по эксплуатации СКЗИ.

Подключение и обеспечение обмена информации с виртуальными частными сетями, принадлежащим сторонним организациям, возможно при условии принятия обеими сторонами соглашении о неразглашении передаваемой информацией.

Подключение к виртуальным частным сетям не должно приводить к снижению уровня защиты информации в виртуальных частных сетях Учреждения.

5.10.4. Компрометация ключей

Все действия по обеспечения сохранности ключей должны быть направлены на исключение компрометации ключей или, по крайней мере, сведении неявной компрометации к явной компрометации.

В случае компрометации ключей или подозрения на компрометацию пользователь обязан прекратить любое использование СКЗИ и незамедлительно сообщить о данном факте в отдел по защите информации.

5.11. Использование мобильных устройств

Под мобильным устройством понимается любое устройство обработки информации в электронном виде, по особенностям своей конструкции, предназначенные для обработки информации без привязки к определенному месту (ноутбуки, планшеты, видеокамеры, смартфоны и т.п.).

Использование работниками личных мобильных устройств для выполнения должностных обязанностей запрещено (за исключением случаев совершения телефонных звонков по личным сотовым телефонам).
Подключение личных мобильных устройств к локальным вычислительным сетям Учреждения запрещено.
Служебные мобильные устройства должны отвечать требованиям настоящей Политики, включая требования по парольной защите, антивирусной защите, установленному программному обеспечению, использованию СКЗИ, использования технологий беспроводной передачи данных и т.п. Служебные мобильные устройства, не отвечающих требованиям настоящей Политики, запрещено использовать для выполнения должностных обязанностей работниками, в том числе подключать их к локальным вычислительным сетям Учреждения.
Обработка информации ограниченного доступа на мобильных устройствах должна соответствовать требованиям нормативно-правовых актов Российской Федерации, Сахалинской области и организационно-распорядительных документов Учреждения.
Работник, использующий служебные мобильные устройства, несет персональную ответственность за обеспечение их сохранности. Работникам запрещено создавать предпосылки для осуществления утраты, кражи и иных противоправных действий со служебными мобильными устройствами.
Использование служебных мобильных устройств в личных целях, а также для совершения противоправных действий запрещено.

5.12. Использование отчуждаемых устройств

В целях настоящей Политики под отчуждаемыми устройствами будут пониматься носители информации, подключаемые к устройствам обработки информации (флэш-диски, устройства, содержащие карты памяти, накопители большой емкости и т.п.).
Работников, которым необходимо использование отчуждаемых носителей информации для выполнения должностных обязанностей, Учреждение должно обеспечить такими носителями. Использование личных отчуждаемых носителей информации работников для выполнения должностных обязанностей разрешено, при условии выполнения требований настоящей Политики. Необходимость использования работником личных отчуждаемых носителей информации должна быть сведена к минимуму, путем обеспечения работников служебными отчуждаемыми носителями информации.
Служебные отчуждаемые носители информации должны подлежать учету, а их передача работникам должна быть подтверждена их подписью. Работник несет персональную ответственность за их сохранность. Работникам запрещено создавать предпосылки для осуществления утраты, кражи и иных противоправных действий со служебными отчуждаемыми носителями информации.
Использование отчуждаемых носителей информации для хранения информации ограниченного доступа должно соответствовать требованиям нормативно-правовых актов Российской Федерации, Ростовской области и организационно-распорядительных документов Учреждения.
Использование служебных отчуждаемых носителей информации в личных целях запрещено.
Подключение отчуждаемых носителей информации к техническим средствам, заведомо содержащим вирусы и/или вредоносные программы, запрещено.
Эксплуатация отчуждаемых носителей информации должна осуществляться в соответствии с рекомендациями производителя по их эксплуатации, и направлена на предупреждение их неисправности.
Каждый отчуждаемый носитель имеет уникальный номер тома. При форматировании носителя номер тома меняется. В связи с чем самостоятельное форматирование служебных отчуждаемых носителей пользователям запрещено.

5.13. Обеспечение сетевой безопасности

Конфигурация и настройка всех устройств, подключенных к локальным вычислительным сетям Учреждения, должны соответствовать требованиям нормативно-правовых актов Российской Федерации и организационно-распорядительным документам Учреждения.
Размещение в локальных вычислительных сетях Учреждения информации ограниченного доступа должно соответствовать требованиям нормативно-правовых актов Российской Федерации и организационно-распорядительным документам Учреждения.
Используемые внешние интерфейсы и протоколы локальных вычислительных сетей Учреждения должно быть максимально ограничены таковыми, необходимыми для обеспечения выполнения Учреждения своих задач и функций.
Технические средства, обеспечивающие работу локальных вычислительных сетей, в том числе демилитаризованных зон, должны размещаться с соблюдением требований по контролю физического доступа к ним и организации их сохранности. Доступ в помещения лиц, не уполномоченных для работы с данным оборудованием, должен быть исключен или осуществляться в сопровождении уполномоченных работников Учреждения.
Использование для подключения и управления техническими средствами протокола Telnet запрещено. Для управления техническими устройствами в сети по возможности должен быть использован протокол SSH.

5.13.1. Построение локальных вычислительных сетей Учреждения

Построение и управление локальными вычислительными сетями должно исключать наличие «узких мест», нарушение работы которых приведет к нарушению работы всей локальной вычислительной сети.
Построение и управление каналов связи локальной вычислительной сети должно обеспечивать возможность осуществления нормальной работы локальной вычислительной сети при нарушении работоспособности основного канала связи.
Все локальные вычислительные сети Учреждения должны быть настроены для недопущения несанкционированного подключения к ним и обнаружения попыток таких подключений.
Подключение к локальным вычислительным сетям Учреждения разрешено только после выполнения требований настоящей Политики и критериев, определяемых Учреждением.
Доступ к информации о системе внутренней адресации в локальных вычислительных сетях, конфигурации и иной подобной информация должен быть обусловлен только выполнением должностных обязанностей. В отдельных случаях, подобная информация может предоставляться третьим лицам, для проведения работ в рамках договорных обязательств. При этом между сторонами должно быть заключено соглашение о конфиденциальности.
Все сервера Учреждения должны быть логически выделены в отдельную подсеть с использованием технологий построения подсетей межсетевыми экранами или иным оборудованием.
Использование любого типа подключений (DSL-модем, dial-up модем, модемы, использующие сети операторов мобильной связи и т.п.) технических средств, размещенных в локальных вычислительных сетях Учреждения, к внешним информационным ресурсам, запрещено без согласования с уполномоченными работниками Учреждения. Такие подключения должны соответствовать требованиям нормативно-правовых актов Российской Федерации и организационно-распорядительным документам Учреждения.
Из каталогов общего доступа в локальных вычислительных сетях Учреждения уполномоченные работники должны регулярно уничтожать не требуемые файлы.

5.13.2. Организация коммутируемого доступа в локальные вычислительные сети Учреждения

Все входящие коммутируемые подключения, имеющие подключения к внутренним ресурсам локальных вычислительных сетей Учреждения, должны подключаться с применением дополнительных мер контроля доступа. Доступ через коммутируемые

подключения к внутренним ресурсам локальных вычислительных сетей Учреждения должен быть максимально ограничен только требуемыми информационными ресурсами.
Телефонные номера для организации коммутируемых подключений не должны публиковаться в открытых информационных ресурсах или иным образом предоставляться третьим лицам без согласования с Министерством здравоохранения Сахалинской области.
Модемы, используемые для организации входящих коммутируемых подключений, должны быть настроены соответствующим образом для начала обработки входящего подключения только после четвертого звонка.
При наличии технической возможности телефонные номера для организации коммутируемых подключений должны ежегодно изменяться.

5.13.3. Организация межсетевого взаимодействия с третьими лицами

Договоры с третьими лицами о предоставлении услуг, требующих подключение к локальным вычислительным сетям Учреждения, должны содержать требования о, как минимум, соответствии уровня защиты таких подключений уровню защиты локальных вычислительных сетей Учреждения.
Установление подключения локальных вычислительных сетей и отдельных автоматизированных рабочих мест третьих лиц к локальным вычислительным сетям Учреждения допускается только по согласованию с отделом системного программного обеспечения и сетевых технологий Учреждения. Такие подключения должны соответствовать требованиям нормативно-правовых актов Российской Федерации и организационно-распорядительным документам Учреждения.
Учреждение обязано вести реестр сторонних подключений к локальным вычислительным сетям Учреждения.

5.13.4. Обеспечение безопасности маршрутизаторов

Настройка маршрутизаторов должна осуществляться в соответствии с рекомендациями производителя, обеспечивающими максимальный уровень безопасности.
Создание локальных учетных записей на маршрутизаторах запрещено. Для аутентификации пользователей должен использоваться протокол TACACS+.
Доступ к настройкам маршрутизатора должен быть ограничен паролем, отвечающим требованиям к организации парольной защиты Учреждения.
Добавление прав правил маршрутизации должно осуществляться на основании настоящей Политики Учреждения и позволять решать задачи и функции, возложенные на Учреждение. Правила маршрутизации должны быть утверждены директоромУчреждения и находиться у уполномоченного на администрирование маршрутизаторов работника.

5.13.5. Использование официальных сайтов

Оплата и заключение договоров на регистрацию доменных имен, для всех официальных web-сайтов Учреждения, должны производиться своевременно и в соответствии с требованиями нормативно-правовых актов Российской Федерации.
Перед предоставлением публичного доступа к web-сайта, при наличии возможности, должен быть проведен анализ защищенности web-сайта и внесены изменения, направленные на обеспечение его максимальной защищенности.

5.13.6. Ограничения по использованию локальных вычислительных сетей Учреждения

Пользователям запрещен просмотр информационных ресурсов Учреждения, содержащихся на автоматизированных рабочих местах других пользователей или в локальных вычислительных сетях Учреждения, если это не обусловлено выполнением должностных обязанностей.
Пользователям запрещено выполнение команд уровня операционной системы или предпринимать попытки их выполнения. Действия пользователя должны быть ограничены взаимодействием с элементами экранных форм программного обеспечения, необходимым для выполнения должностных обязанностей.

При увольнении или изменении должностных обязанностей пользователя, файлы, содержащиеся на его автоматизированном рабочем месте, должны быть проверены его непосредственным руководителем и, в случае необходимости, переданы другим исполнителям.

5.14. Управление доступом к ресурсам

Работникам Учреждения запрещено осуществление противоправных действий, включая, деятельность по получению несанкционированного доступа к любой информационной системе; нанесение ущерба и нарушение работы информационных систем; перехват паролей или иной способ получения паролей, ключевой информации или иных механизмов доступа, которые могут быть использованы для несанкционированного доступа.

Программное обеспечение, предполагающее использование механизмов разделения доступа или подразумевающее индивидуальную ответственность работника за осуществляемые действия, должно использовать механизм контроля доступа, с идентификацией и авторизацией пользователя с помощью, как минимум пароля, отвечающего требованиям к организации парольной защиты.

Доступ к информации ограниченного доступа должен соответствовать требованиям нормативно-правовых актов Российской Федерации.

Меры безопасности, используемые на автоматизированных рабочих местах и в локальных вычислительных сетях, должны быть просты для использования, управления и аудита.

Настройка доступа ко всем информационным ресурсам Учреждения должна быть по умолчанию направлена на предотвращение к ним любого несанкционированного доступа.

Если система контроля доступа автоматизированного рабочего места, локальной вычислительной сети или информационной системы вышла из строя, то по умолчанию доступ пользователей должен быть запрещен.

До предоставления прав доступа к информационным ресурсам Учреждения, пользователь должен быть ознакомлен под роспись с нормативно-правовыми актами Российской Федерации и организационно-распорядительными документами Учреждения, регламентирующими работу с конкретными информационными ресурсами. В случаях, когда это определено необходимостью или требованиями нормативно-правовых актов Российской Федерации, или организационно-распорядительными документами Учреждения должен быть проведен дополнительный инструктаж или обучение. Факт проведения инструктажа или обучения должен быть закреплен в соответствии с требованиями документов, обуславливающих их проведение.

В случаях, когда это определено нормативно-правовыми актами Российской Федерации и организационно-распорядительными документами Учреждения, работник помимо ознакомления, должен письменно подтвердить свое обязательство выполнять требования документов.

5.14.1. Общие правила доступа к локальным вычислительным сетям Учреждения

Доступ к информационным ресурсам Учреждения должен осуществляться согласно разработанной уполномоченным работником и утвержденной директором «Разрешительной системы», составленной исходя из необходимости выполнения должностных обязанностей работниками Учреждения.

В «Разрешительной системе» должны быть отражены все пользователи Учреждения, имеющие доступ к информационным ресурсам Учреждения.

Любое изменение в правах доступа к информационным ресурсам Учреждения должно быть обосновано выполнением должностных обязанностей, утверждено и направлено в письменном виде уполномоченным работникам.

Запрещено предоставление доступа к информационным ресурсам Учреждения, до утверждения такого доступа, уполномоченным работником.

В Учреждения должна вестись и своевременно обновляться «Разрешительная система» к информационным ресурсам Учреждения.

При увольнении работников Учреждения или изменении их должностных обязанностей, лица, уполномоченные на предоставление прав доступа, должны быть письменно проинформированы в трехдневный срок, после чего внести соответствующие изменения в систему контроля доступа и «Разрешительную систему».

5.14.2. Идентификатор учетной записи

Идентификатор учетной записи пользователя должен быть составлен таким образом, чтобы не позволить не уполномоченным лицам установить личность пользователя по своему составу.

Для установления персональной ответственности идентификатор учетной записи пользователя в любой информационной системе должен однозначно соответствовать отдельному работнику.

Для доступа к автоматизированному рабочему месту и локальной вычислительной сети Учреждения у каждого пользователя должны быть уникальный набор из идентификатора учетной записи и пароля. Запрещено создание идентификатора учетной записи, используемого группой лиц.

Использование идентификатора учетной записи пользователя после увольнения или прекращения использования информационных ресурсов Учреждения запрещено.

При предоставлении идентификатора учетной записи сторонним организациям необходимо заключение соглашений, подтверждающих обязательства сторонних организаций соблюдать требования нормативно-правовых актов Российской Федерации и организационно-распорядительных документов Учреждения, подписанные уполномоченными работниками.

При прекращении необходимости использования сторонними компаниями идентификатора учетной записи, лица, уполномоченные на предоставление прав доступа, должны быть письменно проинформированы в однодневный срок, после чего внести соответствующие изменения в систему контроля доступа и «Разрешительную систему».

Для всех лиц, не являющихся служащими Учреждения, но для выполнения обязательств которых, необходимо предоставление доступа к автоматизированным рабочим местам и локальным вычислительным сетям Учреждения, должен быть сформирован идентификатор учетной записи, действующий только на период выполнения лицом своих обязательств. В случае, если срок выполнения обязательств не определен, то срок действия идентификатора учетной записи должен составлять 15 дней.

Пользователям запрещено использование идентификаторов учетных записей и паролей, используемых для получения доступа к информационным ресурсам Учреждения, для идентификации и аутентификации на публичных ресурсах СОП.

5.14.3. Учетные записи специальных типов

Все информационные системы и технические средства, используемые в Учреждении, должны поддерживать специальный тип учетной записи, позволяющий производить любые поддерживаемые настройки и изменения, включая изменения в системе обеспечения безопасности.

Количество таких типов учетных записей должно быть максимально ограничено и предоставлено только тем пользователям, которым это необходимо для осуществления должностных обязанностей с учетом соблюдения требований нормативно-правовых актов Российской Федерации и организационно-распорядительных документов Учреждения.

Таким лицам должно быть предоставлены как минимум два типа учетных записей, одна – специальный тип учетной записи, другая – ограниченный тип учетной записи для повседневной работы, не требующей изменения настроек информационной системы.

Удаленное администрирование любых технических устройств в локальных вычислительных сетях органов Учреждения, при котором осуществляется передача информации через сети общего пользования запрещено.

5.14.4. Требования по настройке системы управления доступом

Автоматизированные рабочие места должны автоматически переходить в режим запроса пароля после определенного периода бездействия или при отсутствии возможности контроля пользователем доступа к автоматизированному рабочему месту.
При наличии технической возможности, средства контроля доступа должны быть настроены на временную блокировку доступа к ним, после трехкратной попытки получения доступа, и уведомления уполномоченных лиц о таковых фактах.
При наличии технической возможности удаленные подключения к информационным системам Учреждения должны автоматически отключаться после определенного времени неактивности такого подключения.
Пользователям запрещено собирать и копировать информацию из информационных ресурсов, если это не обусловлено выполнением должностных обязанностей. При наличии технической возможности используемые системы контроля доступа должны предупреждать возможность таких действий и информировать о таких попытках.

5.14.5. Требования безопасности по использованию системы управления доступа

Работникам запрещено устанавливать и использовать программное обеспечение, направленное на обход установленных механизмов доступа или получение сведений для несанкционированного доступа. Если использование такого программного обеспечения необходимо для выполнения должностных обязанностей, то его использование должно осуществляться по согласованию с отделом системного программного обеспечения и сетевых технологий, а также с отделом по защите информации.

5.15. Управление персоналом

В соответствии с нормативными правовыми актами Российской Федерации конкретные требования по обеспечению информационной безопасности должны быть внесены в должностные регламенты всех работников Учреждения, в зависимости от их должностных обязанностей.
Подбор, и порядок вступления в договорные и трудовые отношения и их расторжения, а также ежедневное выполнение работником его должностных обязанностей, должны соответствовать требованиям нормативно-правовых актов Российской Федерации и организационно-распорядительной документации Учреждения.
Порядок допуска работника к работе с информацией ограниченного доступа, порядок работы с такой информацией и порядок прекращения допуска к такой информации, должен соответствовать требованиям нормативно-правовых актов Российской Федерации и организационно-распорядительной документации Учреждения.

5.15.1. Требования до приема на работу

Претендентам на работу не должна раскрываться информация об имеющейся системе защиты информации.
До начала выполнения своих должностных обязанностей до претендента должны быть доведена вся необходимая информация и проведены все инструктажи в соответствие с требованиями к дисциплинарной, административной и уголовной ответственности в соответствии с требованиями нормативно-правовых актов Российской Федерации и организационно-распорядительной документации Учреждения.

5.15.2. Требования при выполнении должностных обязанностей

Ответственное выполнение требований по информационной безопасности является обязанностью всех работников Учреждения. Требования по информационной безопасности касаются всех работников Учреждения.
Для выполнения требований по информационной безопасности работники должны знать требования нормативно-правовых актов Российской Федерации и организационно-распорядительной документации Учреждения, регламентирующие данные требования и письменно подтверждать свое согласие на их выполнение.
В зависимости от должностных обязанностей, знание требований по информационной безопасности могут быть включены в программу проведения аттестации персонала.

Поведение работников должно соответствовать Этическому кодексу работника Учреждения.
Употребление алкоголя, наркотиков и иных запрещенных препаратов на рабочем месте запрещено, кроме случаев, когда это производится в соответствии с медицинскими показателями и не противоречит требованиям нормативно-правовых актов Российской Федерации и организационно-распорядительной документации Учреждения.
Невыполнение требований нормативно-правовых актов Российской Федерации и организационно-распорядительной документации Учреждения по информационной безопасности является поводом для проведения служебных расследований и возможному привлечению к дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством Российской Федерации и административно-правовыми нормами, установленными в Учреждения.
Для выполнения требований по информационной безопасности пользователям запрещено прибегать к помощи третьих лиц, без согласования с уполномоченными лицами.
Раскрытие сведений о финансовом состоянии работников должно осуществляться в соответствии с требованиями нормативно-правовых актов Российской Федерации и организационно-распорядительной документации Учреждения.

5.15.3. Требования при прекращении выполнения должностных обязанностей

При увольнении или прекращении договорных обязательств работники должны быть уведомлены и согласны с требованиями по неразглашению информации ограниченного доступа и сведений о системе защиты информации, в соответствии с требованиями нормативно-правовых актов Российской Федерации и организационно-распорядительной документации Учреждения.
При увольнении работник обязан передать уполномоченным работникам Учреждения все материальные ценности Учреждения, предоставленные ему для выполнения должностных обязанностей.

5.16. Повышение осведомленности персонала в области информационной безопасности

Проведение мероприятий, направленных на постоянное повышение осведомленности работников Учреждения в области информационной безопасности, должно являться одной из задач, решаемых Учреждением.
Такие мероприятия могут в себя включать, но не ограничиваться, созданием телевизионных роликов, печатных материалов, компьютерных программ, содержащих информацию об обеспечении информационной безопасности в доступной форме, проведение массового обучения, в том числе и без отрыва от рабочего места, периодическую проверку знаний и т.п.
Необходимо проведение периодического практического тестирования готовности работников к выполнению своих должностных обязанностей по защите информации.
Работник, чьи должностные обязанности предполагают выполнение работ по созданию, настройке, сопровождению и совершенствованию системы по обеспечению информационной безопасности, должны проходить специализированное обучение по данным направлениям.

5.17. Обеспечение информационной безопасности при взаимодействии с третьими лицами

В данном разделе настоящей Политики рассмотрено два типа информации. Первый тип – информация, разрешенная к передаче третьим лицам, включая информацию, передаваемую для выполнения требований нормативно-правовых актов Российской Федерации и Ростовской области и информацию, определенную как общедоступная. Второй тип - информация, возможность и требования к передаче третьим лицам которой не определена.
При передаче информации третьим лицам работник обязан выполнять требования по такой передаче, определенные нормативно-правовыми актами Российской Федерации,

Ростовской области и владельцем информации. Дополнительно работник обязан уточнять требования настоящей Политики для конкретных ситуаций, обусловленных выполнением его должностных обязанностей. В случае невозможности самостоятельного определения возможности и требований к передаче информации третьим лицам, работник обязан обратиться к директору Учреждения за уточнением.

5.17.1. Требования к передаче информации

К передаче информации третьим лицам допускается только достоверная информация (за исключением случаев, предусмотренных нормативно-правовыми актами Российской Федерации). При существенных изменениях информации, уже переданной третьим лицам, необходимо их уведомления об изменениях (особенно в случаях, когда переданная информация используется для принятия решений).

При передаче информации третьим лицам должен быть указан автор информации (или ее владелец), номер передаваемой версии (в случае если существует несколько версий), а также лицо, санкционировавшее передачу и дату передачи. Также могут быть нанесены утвержденные нормативно-правовыми актами Российской Федерации обозначения, указывающие на ограничения при использовании передаваемой информации (гриф секретности и т.п.)

Оформление и порядок передачи информации третьим лицам должен осуществляться в соответствии с требованиями по оформлению и ведению делопроизводства, принятыми в правительстве Ростовской области.

5.17.2. Ограничения при передаче информации

Информация второго типа не должна передаваться третьим лицам без возникновения необходимости их ознакомления с такой информацией. При этом порядок передачи такой информации должен соответствовать требованиям нормативно-правовых актов Российской Федерации, Ростовской области и согласован с уполномоченным работником Учреждения.

Передача информации второго типа лицам, временно исполняющим обязанности работников, персоналу компаний, состоящих в договорных обязательствах с Учреждением и другим третьим лицам, должна осуществляться после санкционирования такой передачи уполномоченным лицом Учреждения (путем письменного распоряжения или иным легитимным способом) и, в случае необходимости, заключения соглашения о конфиденциальности или иного документа, содержащего требования о неразглашении получаемой информации.

Работникам запрещено передавать кому бы то ни было информацию, принадлежащую третьим лицам, без соответствующего разрешения с их стороны.

5.17.3. Передача информации третьих лиц

Все запросы третьих лиц, о предоставлении информации второго типа, должны быть переданы уполномоченным работникам Учреждения.

5.17.4. Размещение информации в общедоступных ресурсах

Ведение работниками Учреждения блогов, публикации в электронных форумах, комментарии на общедоступных ресурсах должны соответствовать требованиям организационно-распорядительных документов Учреждения. Такие публикации не должны раскрывать сведения, содержащие информацию ограниченного доступа.

5.17.5. Несанкционированная передача информации

В случае несанкционированной передачи информации третьим лицам, работник, обнаруживший факт такой передачи, должен немедленно уведомить отдел по защите информации. Уполномоченный работник Учреждения должен принять меры в соответствии с требованиями нормативно-правовых актов Российской Федерации, Ростовской области и организационно-распорядительных документов Учреждения.

5.18. Обеспечение соответствия информационной безопасности требованиям нормативно-правовых актов Российской Федерации

Деятельность по обеспечению информационной безопасности в Учреждении должна соответствовать таковым требованиям, предъявляемым нормативно-правовыми актами Российской Федерации.

Обработка информации ограниченного доступа должна осуществляться в соответствии с требованиями нормативно-правовых актов Российской Федерации и Учреждения в зависимости от ее уровня конфиденциальности.

Разрабатываемые в Учреждении организационно-распорядительные документы по обеспечению информационной безопасности не должны противоречить требованиям нормативно-правовых актов Российской Федерации и Учреждения.

Лица, ответственные за работу с кадрами в Учреждении, должны обеспечить ознакомление всех работников с требованиями нормативно-правовых актов Российской Федерации и организационно-распорядительными документами Учреждения, в соответствии с их должностными обязанностями.

При выполнении своих должностных обязанностей работники Учреждения должны в полной мере выполнять требования настоящей Политики. Проверка выполнения требований возлагается на уполномоченных работников Учреждения.

Работники обязаны соблюдать требования, обусловленные договорными обязательствами, указанные в лицензионных соглашениях, соглашениях с третьими лицами, по соблюдению авторских прав и иные законные требования, возникающие в ходе выполнения должностных обязанностей.

6. Ответственность

Ответственность за нарушение требований настоящей Политики накладывается на работников Учреждения, подразумевающих исполнение требований настоящей Политики, совершивших нарушения, в зависимости от категории нарушения, возникшего в результате необеспечения или нарушения требований настоящей Политики, и величины причиненного ущерба (нежелательных последствий).

Указанные категории лиц могут привлекаться к дисциплинарной ответственности.