УТВЕРЖДАЮ

Директор ООО «Югра Смарт Сервис»

_____ А.В. Задимидченко

«___»_____2017 г.

**ПОЛОЖЕНИЕ**

**О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИИ РАБОТ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ**

**в ООО «Югра Смарт Сервис»**

# СОДЕРЖАНИЕ

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

*Автоматизированная система (АС)* - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

*Администратор АС* - лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.

*Администратор безопасности АС* - лицо, ответственное за защиту АС от несанкционированного доступа к информации.

*Вспомогательные технические средства и системы (ВТСС)* - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

*Информационная система персональных данных (ИСПДн)* - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

*Информационные технологии* - процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов.

*Контролируемая зона (КЗ)* - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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

*Несанкционированный доступ (несанкционированные действия) (НСД)* - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим техническим характеристикам и функциональному предназначению.

*Объект информатизации* - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

*Персональные данные (ПДн)* - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, вероисповедание, национальность, другая информация.

*Побочные электромагнитные излучения и наводки (ПЭМИН)* - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

*Средства вычислительной техники (СВТ)* - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

*Система защиты информации* - совокупность органов и (или) исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

*Технические средства информационной системы персональных данных (ТСИСПДн)* - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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, приложения и т. п.), средства защиты информации.

# 1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о порядке организации и проведения работ по обеспечению безопасности конфиденциальной информации (далее - КИ) при их обработке в учреждении (далее - Положение) относится к основополагающим документам, определяющим общие принципы организации работ по информационной безопасности КИ в ООО «Югра Смарт Сервис». Положение разработано в соответствии с Федеральным законом от 08.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», руководящим документом (РД) «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» — Гостехкомиссия России, 1992 год, РД Специальные требования и рекомендации по технической защите конфиденциальной информации (СТРК) — Гостехкомиссия России, 2002 год, РД «Защита от несанкционированного доступа к информации» Термины и определения — Гостехкомиссия России, 1992.

1.2. Организация и проведение работ по обеспечению безопасности информации, содержащей КИ, на объектах информатизации ООО «Югра Смарт Сервис» проводится на основании законодательных и нормативных актов Российской Федерации в области защиты информации и настоящего Положения.

1.3. Требования настоящего Положения являются обязательными для исполнения в ООО «Югра Смарт Сервис», а также организациями, учреждениями и предприятиями, выполняющими работы по защите информации в ООО «Югра Смарт Сервис».

1.4. Положение определяет порядок организации и проведения работ по защите информации, содержащей КИ, на объектах информатизации ООО «Югра Смарт Сервис» как в период их создания, так и в процессе повседневной эксплуатации.

1.5. Принимаемые меры по защите информации на объектах информатизации ООО «Югра Смарт Сервис» должны обеспечивать выполнение действующих требований и норм по защите информации.

1.6. Разработка мер и обеспечение защиты информации на объектах информатизации осуществляются отделом информатизации ООО «Югра Смарт Сервис» или ответственным за защиту информации работником.

Разработка мер защиты информации может осуществляться также сторонними организациями, имеющими лицензии ФСТЭК России и ФСБ России на право проведения соответствующих работ.

Согласование планируемых мер, контроль выполнения работ на местах, соответствия принятых мер и проводимых мероприятий по защите информации действующим требованиям и нормам производит отдел информатизации ООО «Югра Смарт Сервис» или ответственный за защиту информации работник.

1.7. Объекты информатизации организации должны соответствовать требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.

1.8. Защита информации организуется в соответствии с действующими нормативными документами ФСТЭК России.

1.9. Ответственность за общее состояние и организацию работ по созданию и эксплуатации объектов информатизации возлагается на начальника отдела информатизации ООО «Югра Смарт Сервис». Ответственность за обеспечение требований по защите информации, циркулирующей на объектах информатизации, возлагается на начальников структурных подразделений организации, эксплуатирующих эти объекты.

1.10. Контроль выполнения требований настоящего Положения возлагается на заместителя директора ООО «Югра Смарт Сервис».

1.11. Финансирование мероприятий по защите информации предусматривается сметами организации на планируемый год. При этом:

- расходы по защите информации при эксплуатации существующих помещений, технических систем и средств включаются в стоимость их содержания;
- затраты, связанные с защитой информации в создаваемых информационно-вычислительных и других технических системах, предусматриваются в стоимости создания и развития этих систем;
- расходы по защите информации при ремонте и реконструкции помещений предусматриваются в стоимости этих работ.

## 2 ОСНОВНЫЕ ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ ОРГАНИЗАЦИИ

2.1. В соответствии с присвоенным классом защищенности АС в организации должен выполняться комплекс организационно-технических мероприятий по защите информации, циркулирующей в помещениях, технических системах и средствах передачи, хранения и обработки информации.

2.2. Накопление, обработка, хранение и передача защищаемой информации в организации происходит на объектах информатизации, которые представляют собой совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения, помещений, в которых они установлены, или помещений, предназначенных для ведения конфиденциальных переговоров.

К объектам информатизации в организации относятся защищаемые помещения и объекты вычислительной техники.

2.3. Целями защиты информации на объектах информатизации организации являются:

- предотвращение утечки информации по техническим каналам;
- предотвращение уничтожения, искажения, копирования, блокирования информации в системах информатизации за счет НСД к ней;
- соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах ее обработки;
- сохранение возможности управления процессом обработки и пользования информацией.

2.4. К основным задачам защиты информации на объектах информатизации организации относятся задачи по предотвращению:

- несанкционированного доведения защищаемой информации до лиц, не имеющих права доступа к этой информации;
- получения защищаемой информации заинтересованным лицом с нарушением установленных прав или правил доступа к защищаемой информации;
- получения защищаемой информации разведкой с помощью технических средств;

- воздействия на защищаемую информацию с нарушением установленных прав или правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

- воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств АС, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

2.5. Защита информации на объектах информатизации ООО «Югра Смарт Сервис» достигается выполнением комплекса организационных мероприятий с применением сертифицированных средств защиты информации от утечки или воздействия на нее по техническим каналам путем НСД к ней, по предупреждению преднамеренных программно-технических воздействий, предпринятых с целью нарушения целостности (модификации, уничтожения) информации в процессе ее обработки, передачи и хранения, нарушения ее доступности и работоспособности технических средств.

## 3. ПОРЯДОК ОПРЕДЕЛЕНИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

3.1. К защищаемой информации организации относится:

- информация, содержащая коммерческую тайну, служебную информацию, ПДн;
- общедоступная информация, уничтожение, изменение, блокирование которой может нанести ущерб ООО «Югра Смарт Сервис».

3.2. По результатам анализа информации, обрабатываемой в ООО «Югра Смарт Сервис» составляются:

- «Список сотрудников, допущенных к обработке АС»;
- «Список сотрудников, допущенных в помещение» (с указанием номера помещения);
- «Список сотрудников, ответственных за доступ в помещение» (с указанием номера помещения);

3.3. Защищаемая информация организации может быть представлена:

- на бумажных носителях в виде отдельных документов или дел с документами;
- на машинных носителях в виде файлов, массивов, баз данных, библиотек и пр.;
- в виде речевой информации, при проведении совещаний, переговоров и пр.

3.4. С целью определения технических средств и систем, с помощью которых обрабатывается информация, содержащая КИ, а также помещений, где проводятся обсуждения с использованием такой информации, отделом информатизации или ответственным работником организации составляются и утверждаются перечни технических средств АС и защищаемых помещений.

# 4. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНИЗАЦИИ

4.1. Технический канал утечки информации (ТКУИ) представляет собой совокупность следующих факторов:

- источника информативного сигнала;
- физической среды его распространения;
- приемника, способного зарегистрировать данный сигнал.

4.2. При ведении переговоров и использовании технических средств для обработки и передачи информации на объектах информатизации организации возможна реализация следующих ТКУИ:

- акустического излучения информативного речевого сигнала;
- электрических сигналов, возникающих при преобразовании информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющихся по проводам и линиям, выходящим за пределы КЗ;
- НСД к обрабатываемой в АС информации и несанкционированные действия с ней;
- воздействия на технические или программные средства АС в целях нарушения конфиденциальности, целостности и доступности информации посредством специально внедренных программных средств;
- ПЭМИН информативных сигналов от технических средств АС и линий передачи информации;
- наводок информативного сигнала, обрабатываемого техническими средствами АС, на цепи электропитания и линии связи, выходящие за пределы КЗ;
- радиоизлучений, модулированных информативным сигналом, возникающим при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;
- радиоизлучений или электрических сигналов от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации («закладочные устройства»), модулированных информативным сигналом;

- радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;
- просмотра информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;
- прослушивания телефонных и радиопереговоров;
- хищения технических средств с хранящейся в них информацией или носителей информации.

4.3. Перехват информации, циркулирующей на объекте информатизации, или воздействие на нее с использованием технических средств могут вестись:

- из-за границы КЗ из близлежащих строений и транспортных средств;
- из смежных помещений, принадлежащих другим организациям и расположенным в том же здании, что и объект информатизации;
- при посещении организации посторонними лицами;
- за счет НСД к информации, циркулирующей в АС, как с помощью технических средств автоматизированной системы, так и через сети.

4.4. В качестве аппаратуры перехвата или воздействия на информацию и технические средства объекта информатизации могут использоваться портативные возимые и носимые устройства, размещаемые вблизи объекта либо подключаемые к каналам связи или техническим средствам обработки информации, а также электронные устройства съема информации - «закладочные устройства», размещаемые внутри или вне защищаемого помещения.

4.5. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны, вследствие:

- непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемого помещения и его инженерно-технических систем;
- некомпетентных или ошибочных действий пользователей;
- непреднамеренного просмотра информации с экранов мониторов и пр.

# 5. ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНИЗАЦИИ

5.1.Защита информации, циркулирующей на объекте информатизации, должна быть комплексной и дифференцированной. С этой целью для каждого объекта информатизации создается система защиты информации.

5.2.Комплексная защита информации на объектах информатизации проводится по следующим основным направлениям работы:

- охрана помещений объекта;
- определение перечня информации, подлежащей защите;
- классификация АС;
- создание системы защиты информации при разработке и модернизации объекта;
- составление организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;
- защита речевой информации при осуществлении конфиденциальных переговоров;
- защита информации, содержащей КИ, при обработке, передаче с использованием технических средств, а также на бумажных или иных носителях;
- защита информации при взаимодействии абонентов с информационными сетями связи общего пользования.

5.3.Перечень необходимых мер защиты информации определяется по результатам обследования объекта информатизации с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения санкционированной доступности и работоспособности технических средств, обрабатывающих эту информацию, а также с учетом реальных возможностей ее перехвата и раскрываемости.

Основное внимание должно быть уделено защите информации, содержащей КИ, в отношении которой угрозы реальны и сравнительно просто реализуемы без применения сложных технических средств перехвата информации. К информации такого рода относится:

- речевая информация, циркулирующая в защищаемом помещении;
- информация, обрабатываемая СВТ;

- информация, выводимая на экраны мониторов;
- документированная информация, содержащая КИ;
- информация, передаваемая по каналам связи, выходящим за пределы КЗ.

5.4.Создание системы защиты информации объекта информатизации осуществляется по следующим стадиям:

- предпроектная стадия, включающая в себя предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания системы защиты конфиденциальной информации (далее СЗКИ) и технического задания на ее создание;
- стадия проектирования (разработки проектов) и реализации АС, включающая в себя разработку СЗКИ в составе объекта информатизации;
- стадия ввода в действие СЗКИ, включающая в себя опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации (далее СрЗИ), а также оценку соответствия АС требованиям безопасности информации (аттестация).

5.4.1. Предпроектная стадия обследования объекта информатизации включает в себя:

- установление необходимости обработки КИ в АС;
- определение КИ, подлежащих защите от НСД;
- определение условий расположения технических средств АС относительно границ КЗ;
- определение конфигурации и топологии АС в целом и ее отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- определение технических средств и систем, предполагаемых к использованию в разрабатываемой АС, условий их расположения, общесистемных и прикладных программных средств, имеющихся и предлагаемых к разработке;
- определение режимов обработки КИ в АС в целом и в отдельных ее компонентах;
- определение класса защищенности АС;
- уточнение степени участия должностных лиц в обработке КИ, характер их взаимодействия между собой;

- определение (уточнение) угроз безопасности КИ применительно к конкретным условиям функционирования АС.

5.4.2. По результатам предпроектного обследования на основе документов ФСТЭК России, с учетом установленного класса защищенности АС задаются конкретные требования по обеспечению безопасности КИ, включаемые в техническое (частное техническое) задание на разработку СЗКИ.

5.4.3. Предпроектное обследование может быть поручено специализированной организации, имеющей соответствующую лицензию. Порядок ознакомления (при необходимости) специалистов подрядной организации с защищаемыми сведениями определяется организацией.

5.4.4. Аналитическое обоснование необходимости создания СЗКИ должно содержать:

- информационную характеристику и организационную структуру объекта информатизации;
- характеристику комплекса технических средств АС, программного обеспечения, режимов работы, технологического процесса обработки информации;
- возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;
- перечень предлагаемых к использованию сертифицированных СрЗИ;
- обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации;
- оценку материальных, трудовых и финансовых затрат на разработку и внедрение СЗКИ;
- ориентировочные сроки разработки и внедрения СЗКИ;
- перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации.

Аналитическое обоснование подписывается руководителем организации, проводившей предпроектное обследование, согласовывается с отделом по защите информации или ответственным лицом и утверждается заместителем руководителя организации.

5.4.5. Техническое (частное техническое) задание на разработку СЗКИ должно содержать:

- обоснование разработки СЗКИ;
- исходные данные создаваемой (модернизируемой) АС в техническом, программном, информационном и организационном аспектах;
- класс защищенности АС;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗКИ и приниматься в эксплуатацию АС;
- конкретизацию мероприятий и требований к СЗКИ;
- перечень предполагаемых к использованию сертифицированных СрЗИ;
- обоснование проведения разработок собственных СрЗИ при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных СрЗИ;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗКИ.

5.4.6. В целях дифференцированного подхода к обеспечению безопасности КИ в зависимости от объема обрабатываемых КИ и угроз безопасности важным интересам организации, общества и государства АС подразделяются на классы защищенности.

Класс АС устанавливается в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» — Гостехкомиссия России, 1992, и оформляется актом. Пересмотр класса защищенности АС производится в обязательном порядке, если произошло изменение хотя бы одного из критериев, на основании которых он был установлен.

5.4.7. На стадии проектирования и создания АС (СЗКИ) проводятся следующие мероприятия:

- разработка задания и проекта проведения работ (в том числе строительных и строительно-монтажных) по созданию (реконструкции) АС в соответствии с требованиями технического (частного технического) задания на разработку СЗКИ;
- выполнение работ в соответствии с проектной документацией;
- обоснование и закупка совокупности используемых в АС серийно выпускаемых технических средств обработки, передачи и хранения информации;

- разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;
- обоснование и закупка совокупности используемых в АС сертифицированных технических, программных и программно-технических СрЗИ и их установка;
- проведение сертификации по требованиям безопасности информации технических, программных и программно-технических СрЗИ, в случае когда на рынке отсутствуют требуемые сертифицированные СрЗИ;
- разработка и реализация разрешительной системы доступа пользователей к обрабатываемой на АС информации;
- определение подразделений и назначение лиц, ответственных за эксплуатацию СрЗИ, с их обучением по направлению обеспечения безопасности ПДн;
- разработка эксплуатационной документации на АС и СрЗИ, а также организационно-распорядительной документации по защите информации (распоряжений, инструкций и других документов);
- выполнение других мероприятий, характерных для конкретных АС и направлений обеспечения безопасности КИ.

5.4.8. На стадии ввода в действие АС (СЗКИ) осуществляются:

- выполнение генерации пакета прикладных программ в комплексе с программными СрЗИ;
- опытная эксплуатация СрЗИ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе АС;
- приемо-сдаточные испытания СрЗИ по результатам опытной эксплуатации;
- организация охраны и физической защиты помещений АС, исключающих несанкционированный доступ к техническим средствам АС, их хищение и нарушение работоспособности, хищение носителей информации;
- оценка соответствия АС требованиям безопасности КИ.

# 6. ОТВЕТСТВЕННОСТЬ ДОЛЖНОСТНЫХ ЛИЦ ЗА ОБЕСПЕЧЕНИЕ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ

6.1. Директор ООО «Югра Смарт Сервис» несет ответственность за общую организацию работ по защите информации на объектах информатизации.

6.2. Администратор безопасности ИСПДн ООО «Югра Смарт Сервис» несет ответственность за:

- руководство и координацию работ по защите информации на объектах информатизации;
- организацию выполнения требований по защите информации на объекте информатизации;
- обоснованность необходимости создания СЗКИ объекта информатизации;
- разработку организационно-распорядительных документов по защите информации на объектах информатизации;
- организацию разработки технического задания на создание СЗКИ, подготовку проектов договоров со сторонними организациями на выполнение работ по защите информации на объектах информатизации;
- организацию контроля состояния СЗКИ объекта информатизации, соблюдения работниками установленных норм и требований по защите информации;
- организацию контроля охраны помещений объекта;
- совершенствование СЗКИ.
- сопровождение СЗИ от несанкционированного доступа;
- непосредственное управление режимами работы и административную поддержку функционирования применяемых специальных программных и программно- аппаратных СЗИ от несанкционированного доступа;
- настройку и сопровождение в процессе эксплуатации подсистемы управления доступом;
- проверку состояния используемых СЗИ от несанкционированного доступа, правильности их настройки;
- организацию разграничения доступа;

- учет и контроль состава и полномочий пользователей;

- выполнение требований по обеспечению безопасности при организации технического обслуживания и отправке в ремонт СВТ;

- учет, хранение, прием и выдачу персональных идентификаторов и ключевых дискет ответственным исполнителям;

- контроль учета, создания, хранения и использования резервных и архивных копий массивов данных.

- выбор типа и версии серверных и клиентских операционных систем, установку, настройку, сопровождение операционных систем серверов;

- обновление справочного и антивирусного программного обеспечения;

- реализацию совместно с администратором безопасности сетевой политики безопасности;

- настройку аппаратной и программной составляющей серверного, коммутационного, телекоммуникационного оборудования, средств аппаратной безопасности сегментов, сетевого периферийного оборудования;

- регистрацию пользователей и предоставление им прав доступа к сетевым информационным ресурсам, регистрацию компьютеров в сети;

- реализацию адресной и маршрутной политики сети;

- реализацию политики антивирусной защиты;

- обеспечение работоспособности структурированной кабельной сети;

- архивирование, резервное копирование информации;

- ведение аудита системных событий и безопасности;

- оперативное управление работой сети;

- контроль физической сохранности средств и оборудования сети.

6.3. Работники ООО «Югра Смарт Сервис», эксплуатирующие объект информатизации, несут ответственность за:

- выполнение требований по защите информации на объекте информатизации;

- ведение необходимой документации объекта информатизации;

- правильность определения пользователям своего подразделения необходимости и прав доступа к защищаемым информационным ресурсам.

6.4. Пользователи АС объекта информатизации несут ответственность за:

- соблюдение мер по защите информации и правил эксплуатации СВТ;

- обеспечение сохранности СВТ, машинных носителей информации и целостность установленного программного обеспечения;

- соблюдение установленных требований по обращению с машинными носителями информации.