УТВЕРЖДАЮ
Главный врач ГАУЗ ТО «КДЦ «Эндос»

________________ А.А. Нелаева
________________2016 года

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите конфиденциальной информации в ГАУЗ ТО «Консультативно – диагностический центр «Эндос»

2016 год

Оглавление

		стр.
1.	Общие положения	3
2.	Охраняемые сведения и объекты защиты	5
3.	Организационные и технические мероприятия по защите информации	6
4.	Защита информации автоматизированных рабочих мест на базе автономных ПЭВМ	11
5.	Защита информации при использовании съемных накопителей информации большой емкости для автоматизированных рабочих мест на базе автономных ПЭВМ	12
6.	Защита информации в локальных вычислительных сетях	13
7.	Защита информации при межсетевом взаимодействии	14
8.	Защита информации при работе с системами управления базами данных	14
9.	Возможные технические каналы утечки информации и несанкционированного воздействия на информационные ресурсы и процессы	15
10.	Обязанности и права должностных лиц	17
11.	Контроль состояния защиты информации	19
12.	Планирование работ по защите информации и контролю	22
13.	Аттестация объектов информатизации	23
14.	Взаимодействие с учреждениями и организациями по вопросам защиты информации	25

.

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение определяет цели, задачи, содержание, порядок организации и выполнения мероприятий по защите конфиденциальной информации (некриптографическими методами), направленные на предотвращение ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования (далее именуется - защита информации), в ГАУЗ ТО «Консультативно – диагностический центр «Эндос», (далее ЛПУ).

1.2. Положение является документом, обязательным для выполнения всеми должностными лицами при проведении работ, требующих защиты информации и ПДН, на строящихся (реконструируемых) и действующих (находящихся в эксплуатации) объектах информатизации Учреждения.

1.3. Правовую основу Положения составляют Конституция Российской Федерации, законы Российской Федерации «О безопасности», «Об информации, информационных технологиях и о защите информации», «Об участии в международном информационном обмене», нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» (далее – СТР-К), утвержденный приказом Гостехкомиссии России от 30.08.2002г. № 282 и другие законодательные акты Российской Федерации и Тюменской области, определяющие права и ответственность граждан, общества и государства в сфере информационных отношений. Положение разработано на основе действующих правовых, организационно-распорядительных и нормативных документов по защите информации и детализирует их основные требования применительно к объектам Учреждения.

1.4. Работы по защите информации, обрабатываемой с использованием технических средств, являются составной частью управленческой деятельности ЛПУ Тюменской области и осуществляются во взаимосвязи с работами по другим направлениям обеспечения безопасности. Проведение мероприятий, связанных обсуждением, передачей, обработкой и хранением информации, содержащей сведения конфиденциального характера , допускается только после определения необходимых мер по их защите в соответствии с требованиями настоящего Положения и других нормативно-методических документов по защите информации, представленных в приложении № 1.

1.5. Ответственность за организацию и состояние защиты информации на объектах информатизации возлагается на главного врача ГАУЗ ТО «КДЦ «Эндос». Руководство работами по защите информации осуществляет заместитель главного врача, ответственный за организацию работ по технической защите информации.

Должностные лица, организующие работу с информацией конфиденциального характера, несут персональную ответственность за соблюдение требований настоящего Положения.

В целях руководства разработкой и осуществлением мероприятий по обеспечению защиты конфиденциальной информации на объектах информатизации и проведения постоянного контроля за ее состоянием, в Учреждении назначается ответственный по защите информации, подчиненный первому заместителю главного врача − ответственному за организацию и руководство работами по защите информации на объектах информатизации в Учреждении.

Функции и права ответственного по защите информации определяются Инструкцией ответственному по защите информации, утверждаемой главным врачом.

Ответственный по защите информации осуществляет мероприятия по защите информации, участвует в согласовании технических заданий при разработке системы защиты информации или ее отдельных компонентов специализированными организациями на строительство (реконструкцию) объектов информатизации Учреждения, создании систем информатизации и связи и организует контроль эффективности мероприятий, осуществляемых в интересах обеспечения защиты конфиденциальной информации в Учреждении.

При решении задач, связанных с защитой информации конфиденциального характера, ответственный по защите информации взаимодействует с другими подразделениями (специалистами) по защите информации Учреждения.

1.6. Разработка системы защиты информации (далее – СЗИ) может осуществляться как ответственным Учреждения, так и другими специализированными организациями, имеющими лицензии ФСТЭК России на соответствующий вид деятельности.

1.7. Финансирование мероприятий по защите конфиденциальной информации в Учреждении предусматривается ежегодно в сметах расходов на содержание Учреждения. Мероприятия по обеспечению информационной безопасности могут финансироваться в соответствии с областными целевыми программами по защите информации.

1.8 Изменения в текст настоящего Положения вносятся порядком, предусмотренным для его согласования и утверждения. Изменения в приложения к Положению могут вноситься по мере необходимости за подписью первого заместителя директора Учреждения - ответственного за организацию и руководство работами по защите информации в Учреждении.

2. ОХРАНЯЕМЫЕ СВЕДЕНИЯ И ОБЪЕКТЫ ЗАЩИТЫ

2.1. Конфиденциальная информация хранимая, обрабатываемая и циркулирующая на объектах информатизации Учреждения, является критичным ресурсом и требует постоянного поддержания таких ее свойств как конфиденциальность, целостность и доступность, вследствие чего необходимо принятие адекватных мер по обеспечению ее безопасности.

Целью мероприятий по защите конфиденциальной информации, проводимых на объектах информатизации, является снижение риска получения ущерба в условиях действия преднамеренных и непреднамеренных угроз информационной безопасности (в части технической защиты информации). Достижение требуемого уровня защиты конфиденциальной информации должно быть обеспечено системным применением организационных, организационно-технических, технических и программно-технических мер на всех этапах разработки, строительства (реконструкции), испытаний, внедрения и эксплуатации объектов информатизации.

2.2. Указанная цель достигается путем рационального и взаимосвязанного решения на объектах информатизации следующих задач:

• определения и документального оформления перечня сведений, информационных ресурсов и процессов, которые необходимо защитить;

• анализа каналов утечки, хищения, несанкционированного доступа и воздействия на защищаемую информацию;

• оценки возможностей недобросовестных клиентов и криминальных структур по получению защищаемой информации, несанкционированному доступу и воздействию на информационные ресурсы и процессы, оценки реальной опасности утечки информации, искажения, модификации, уничтожения или блокирования информационных ресурсов и процессов;

• разработки и внедрения технически и экономически обоснованных мероприятий по защите информации с учетом выявленных возможных каналов ее утечки, воздействий и доступа;

• организации и проведения контроля эффективности защиты конфиденциальной информации на объектах информатизации Учреждения.

2.3. К охраняемым сведениям, защищаемым информационным ресурсам и процессам на всех этапах жизненного цикла объектов информатизации Учреждения:

2.3.1. Речевая информация, содержащая сведения конфиденциального характера.

2.3.2. Информационные ресурсы, содержащие сведения конфиденциального характера, представленные в виде носителей на магнитной и оптической основе, информативных электрических сигналов, электромагнитных полей, информационных массивов и баз данных.

2.4. При анализе безопасности речевой информации и информационных ресурсов, содержащих сведения конфиденциального характера, должны рассматриваться все возможные виды угроз.

2.5. К объектам информатизации Учреждения, подлежащим защите по требованиям обеспечения безопасности защиты информации, относятся:

2.5.1. Защищаемые помещения, в которых обсуждается информация, содержащая сведения конфиденциального характера, утечка, которой может нанести ущерб Учреждению**,** персоналу, материальным ценностям или отдельным гражданам.

2.5.2. Системы информатизации и связи, предназначенные для обработки информации, содержащей сведения конфиденциального характера:

• локальные вычислительные сети (далее – ЛВС) и отдельные автоматизированные рабочие места (далее - АРМ);

• средства изготовления, размножения и тиражирования документов;

• программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение);

• система звукоусиления и звукозаписи, предназначенная для использования при проведении совещаний по конфиденциальным вопросам;

• средства связи;

• АРМ систем диспетчеризации средств и систем жизнеобеспечения объекта;

• АРМ учрежденческой автоматической телефонной станции.

2.5.3. Вспомогательные технические средства и системы, размещенные в защищаемых помещениях, а также совместно с техническими средствами и системами, обрабатывающими информацию конфиденциального характера.

2.6. Конкретный перечень объектов защиты прилагается (Приложение №5).

3. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

3.1. Защита информации на объектах информатизации Учреждения должна осуществляться посредством выполнения комплекса мероприятий, направленных на: скрытие или существенное затруднение добывания с помощью технических средств защищаемой информации; предотвращение утечки информации или воздействия на информационные ресурсы и процессы по техническим каналам и за счет несанкционированного доступа к ним; предупреждение преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации (информационных технологий) в процессе ее обработки, передачи и хранения или нарушения работоспособности технических средств.

3.2. Исходя из перечня основных угроз информационной безопасности, в комплексе мероприятий по защите информации на объектах информатизации Учреждения определяется несколько направлений:

- защита от утечки по техническим каналам конфиденциальной информации, обсуждаемой в помещениях объектов;
- защита технических средств и систем от утечки информации

конфиденциального характера, по техническим каналам;

- защита конфиденциальной информации, передаваемой по каналам связи (проводным, радио или иным);
- защита информации и информационных процессов (технологий) от несанкционированного доступа, в том числе от компьютерных вирусов и других программно-технических воздействий, от хищения технических средств с находящейся в них информацией или отдельных носителей информации;
- защита информации и информационных процессов (технологий) от воздействия источников дестабилизирующих (разрушающих) электромагнитных излучений, а также от уничтожения и искажения информации через специально внедренные электронные и программные средства (закладки).

3.3. К мероприятиям, скрывающим расположение (технические характеристики) и функциональное назначение (предназначение) помещений (технологического оборудования и технических средств) на этапе эксплуатации можно отнести:

• затруднение возможности перехвата информации, циркулирующей в средствах технологического телевидения и оборудования, за пределами контролируемой зоны объекта информатизации путем локализации средств и оборудования (их линий) в пределах контролируемой зоны, размещения трансформаторной подстанции и контуров заземления на внутренней охраняемой территории Учреждения;

• организацию контроля допуска к проектно-сметной документации объекта информатизации (в том числе к чертежам, пояснительным запискам, макетам, электронным копиям документации и т.д.), уничтожение дополнительно размноженной документации по окончании строительства;

• ограничением количества организаций и их представителей, привлекаемых к работам на объекте информатизации.

3.4. Организация защиты от утечки по техническим каналам конфиденциальной информации в защищаемых помещениях предполагает проведение комплекса организационно-технических мероприятий, направленных на устранение акустического и виброакустического каналов утечки информации, а также технических каналов, возникающих при эксплуатации вспомогательных технических средств и за счет внедрения электронных устройств перехвата информации.

К таким мероприятиям относятся:

3.4.1. Отнесение к защищаемым помещений Учреждения, используемых для обсуждения информации конфиденциального характера.

3.4.2. Проведение специальной проверки защищаемых помещений, а также размещенных в них технических средств иностранного производства с целью выявления возможно внедренных в них электронных устройств перехвата информации (закладок). Специальная проверка технических средств и помещений проводится организациями, имеющими

соответствующие лицензии ФСБ РФ. Необходимость проведения специальной проверки защищаемых помещений, а также установленных в них технических средств иностранного производства определяется соответственно решением главного врача.

3.4.3. Выполнение организационно-режимных мероприятий по допуску и охране защищаемых помещений. Указанные помещения оборудуются замками и запираются на ключ в период между проводимыми мероприятиями и в нерабочее время.

3.4.4. Установка в защищаемых помещениях технических средств (оконечных устройств телефонной связи, радиотрансляции, сигнализации, электрочасофикации и т.д.), сертифицированных по требованиям безопасности информации либо защищенных сертифицированными средствами защиты.

3.4.5. Исключение использования в защищаемых помещениях при проведении конфиденциальных мероприятий радиотелефонов, оконечных устройств сотовой, пейджинговой и транковой связи, незащищенных переносных магнитофонов и других средств аудио и видеозаписи, а также передачи речевой информации по открытым проводным каналам и радиоканалам связи.

При установке в защищаемых помещениях телефонных и факсимильных аппаратов с автоответчиком или спикерфоном, а также телефонных аппаратов с автоматическим определителем номера проводить их отключение от сети на время проведения этих мероприятий.

3.4.6. Выполнение мероприятий по звукоизоляции ограждающих конструкций защищаемых помещений, их систем вентиляции и кондиционирования. Для обеспечения необходимого уровня звукоизоляции помещений рекомендуется оборудование дверных проемов тамбурами с двойными дверями, установка дополнительных рам в оконных проемах, уплотнительных прокладок в дверных и оконных притворах и применение шумопоглотителей на выходах вентиляционных каналов.

Если предложенными выше методами не удается обеспечить необходимую акустическую защиту, следует применять организационные меры, ограничивая на период проведения конфиденциальных мероприятий доступ посторонних лиц в места возможного прослушивания разговоров, ведущихся в защищаемых помещениях.

Для снижения уровня виброакустического сигнала рекомендуется расположенные в защищаемом помещении элементы инженерно-технических систем отопления, вентиляции оборудовать звукоизолирующими экранами.

Для снижения вероятности перехвата информации по виброакустическому каналу рекомендуется организационными мерами исключить возможность установки посторонних предметов на внешней стороне ограждающих конструкций защищаемых помещений и выходящих из них инженерных коммуникаций (систем отопления, вентиляции и кондиционирования).

Если при проведении технического контроля выясняется, что указанные выше меры защиты информации от утечки по акустическому и виброакустическому каналам недостаточны или нецелесообразны, то рекомендуется применять метод активного акустического или виброакустического маскирующего зашумления.

Для этого должны применяться сертифицированные средства активной защиты.

3.4.7. Оформление технических паспортов по вопросам защиты информации на защищаемые помещения осуществляется ответственным по защите информации с привлечением подразделений, эксплуатирующих здания, системы электроснабжения, коммуникации и технические средства, а также подразделений, располагающихся в защищаемых помещениях.

3.4.8. Организация и проведение аттестации защищаемых помещений по требованиям безопасности информации с оформлением «Аттестата соответствия» проводится организациями, имеющими соответствующую аккредитацию ФСТЭК России.

3.5. В целях защиты информации, обрабатываемой всеми видами основных технических средств и систем, организуется и проводится комплекс организационно-технических мероприятий, направленный на обеспечение защиты информации от ее хищения, утраты, утечки, искажения, подделки и блокирования к ней за счет несанкционированного доступа и специальных воздействий, защиты от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

К таким мероприятиям относятся:

3.5.1. Реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к информации и работам, связанным с ее использованием.

3.5.2. Ограничение доступа персонала и посторонних лиц в помещения, где размещены средства информатизации и коммуникационное оборудование, а также хранятся носители информации.

3.5.3. Разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации.

3.5.4. Регистрация действий пользователей ЛВС и АРМ и обслуживающего персонала, контроль несанкционированного доступа и

действий пользователей, обслуживающего персонала и посторонних лиц.

3.5.5. Учет и надежное хранение бумажных и машинных носителей конфиденциальной информации и их обращение, исключающее хищение, подмену и уничтожение.

3.5.6. Использование сертифицированных по требованиям безопасности информации специальных защитных знаков, создаваемых на основе физико-химических технологий для контроля доступа к объектам защиты и для защиты документов от подделки.

3.5.7. Резервирование технических средств, дублирование массивов и носителей информации.

3.5.8. Использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации.

3.5.9. Применение для обработки информации, содержащей сведения конфиденциального характера, технических средств, удовлетворяющих требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности, по санитарным нормам, предъявляемым к видеодисплейным терминалам (ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).

3.5.10. Классификация автоматизированных систем (далее − АС), предназначенных для обработки информации, содержащей сведения, конфиденциального характера, по требованиям защиты от несанкционированного доступа к информации. Переклассификация проводится при изменении хотя бы одного из критериев, на основании которых был установлен класс.

3.5.11. Выполнение требований по защите автоматизированных систем, предназначенных для обработки информации, содержащей сведения, конфиденциального характера, от несанкционированного доступа к информации. Установка и эксплуатация сертифицированной системы защиты информации от несанкционированного доступа. Определение порядка допуска персонала к информации автоматизированной системы, создание системы разграничения доступа пользователей к защищаемым ресурсам, разработка комплекса организационных мер, поддерживающих программно-техническое средство защиты на всех этапах обработки информации и во всех режимах функционирования автоматизированной системы.

Настройка сертифицированного средства защиты от несанкционированного доступа с учетом требований для соответствующего класса. Учет необходимых магнитных носителей информации. Оборудование помещения, в котором размещены средства вычислительной техники, датчиками пожарной и охранной сигнализации и дополнительным замком. Создание условий, исключающих возможность хищения технических средств с хранящейся в них информацией, или отдельных носителей информации. Оборудование окон помещений шторами или жалюзи для исключения возможности просмотра информации с экранов дисплеев и других средств ее отображения с помощью оптических средств. В полном объеме работы проводятся организациями, имеющими соответствующие лицензии ФСТЭК России.

3.5.12. Оформление технических паспортов по вопросам защиты информации на основные технические средства и системы осуществляется работниками подразделения (специалистами) по защите информации совместно с подразделением, эксплуатирующим данные средства.

3.5.13. Организация и проведение аттестации основных технических средств и систем и оформление «Аттестата соответствия» проводится организациями, имеющими соответствующую аккредитацию ФСТЭК России.

3.6. Основными направлениями защиты конфиденциальной информации, передаваемой по каналам связи, выходящим за пределы контролируемой зоны, являются:

• исключение переговоров, содержащих сведения конфиденциального характера, по открытым каналам связи;

• использование при обмене информацией по радиоканалам сигнально-кодовых таблиц;

• использование защищенных каналов связи, в том числе защищенных волоконно-оптических линий связи;

• использование открытых каналов связи с применением криптографических средств защиты информации. Применяемые средства защиты информации должны быть сертифицированы ФСБ РФ (ФАПСИ).

4. ЗАЩИТА ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ НА БАЗЕ АВТОНОМНЫХ ПЭВМ

4.1. Автоматизированные системы могут быть выполнены в виде автоматизированных рабочих мест (АРМ) на базе автономных ПЭВМ с необходимым для решения конкретных задач периферийным оборудованием (принтер, сканер, внешние накопители и т.п.).

Порядок разработки и эксплуатации АРМ на базе автономных ПЭВМ по составу и содержанию проводимых работ в части защиты информации, организационно – распорядительной, проектной и эксплутационной документации должны отвечать требованиям СТР-К.

4.2. Автоматизированные рабочие места на базе автономных ПЭВМ подлежат классификации в соответствии с требованиями руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

5. ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ СЪЕМНЫХ НАКОПИТЕЛЕЙ ИНФОРМАЦИИ БОЛЬШОЙ ЕМКОСТИ ДЛЯ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ НА БАЗЕ АВТОНОМНЫХ ПЭВМ

5.1. Технология обработки информации с использованием съемных накопителей информации большой емкости предусматривает запись на съемный накопитель прикладного программного обеспечения (или его части) и обрабатываемой информации пользователя.

В качестве устройств для работы по этой технологии могут быть использованы как встроенные (съемные), так и выносные накопители на магнитных, магнитно-оптических дисках различной конструкции.

Одновременно может быть установлено несколько съемных накопителей информации большой емкости.

Основной особенностью применения такой технологии для АРМ на базе автономных ПЭВМ, с точки зрения защиты информации, является исключение хранения информации на ПЭВМ в нерабочее время.

Эта технология может быть использована для обработки защищаемой информации без применения сертифицированных средств защиты информации от несанкционированного доступа и использования средств физической защиты помещений.

5.2. На стадии предпроектного обследования проводится детальный анализ технологичного процесса обработки информации, обращается внимание, прежде всего, на технологию обмена информацией (при использовании съемных накопителей информации большей емкости или гибких магнитных дисков) с другими АРМ, как использующими, так и не использующими эту технологию, на создание условий, исключающих запись информации на неучтенные носители информации, несанкционированное ознакомление с этой информацией, на организацию выдачи информации на печать.

5.3. Обмен конфиденциальной информацией между АРМ должен осуществляться только на учтенных носителях информации с учетом допуска исполнителей, работающих на АРМ, к передаваемой информации.

5.4. На рабочих местах исполнителей, работающих по этой технологии, во время работы не должно быть неучтенных накопителей информации.

В случае формирования конфиденциальных документов с использованием открытой текстовой и графической информации, представленной на накопителях информации, такие накопители информации должны быть «закрыты на запись».

Условия и порядок применения таких процедур должны быть отражены в технологии обработки информации.

5.5. При использовании в этой технологии современных средств вычислительной техники, оснащенных энергозависимой, управляемой извне перезаписываемой памятью, перед началом работ с конфиденциальной информацией при загрузке ПЭВМ рекомендуется выполнять процедуру проверки целостности перезаписываемой памяти. При обнаружении нарушения целостности перезаписываемой памяти необходимо поставить об этом в известность руководителя подразделения и ответственного по защите информации.

5.6. На рабочем месте должна быть разработана и по согласованию с ответственным по защите информации утверждена главным врачом Учреждения, технология обработки конфиденциальной информации, использующая съемные накопители информации большой емкости и предусматривающая выполнение требований по защите информации, учитывающих условия размещения, эксплуатации АРМ, учет носителей информации, а также другие требования, вытекающие из особенностей функционирования АРМ.

6. ЗАЩИТА ИНФОРМАЦИИ В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

6.1. Характерными особенностями ЛВС являются распределенное хранение информации, ее удаленная обработка и передача, а также сложность проведения контроля за работой пользователей и общей защищенностью ЛВС.

6.2. Конфиденциальная информация может обрабатываться только в ЛВС, расположенных в пределах контролируемой зоны и оборудованных межсетевыми экранами.

6.3. Средства защиты информации от несанкционированного доступа должны использоваться во всех узлах ЛВС независимо от наличия (отсутствия) сведений конфиденциального характера в данном узле ЛВС и требуют постоянного квалифицированного контроля настроек СЗИ администратором защиты информации.

6.4. Класс защищенности ЛВС определяется в соответствии с требованиями руководящего документа ФСТЭК России (Гостехкомиссия) «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

6.5. Для управления, контроля защищенности ЛВС и распределения системных ресурсов в ЛВС, включая управление средствами защиты информации, обрабатываемой (хранимой, передаваемой) в ЛВС, должны использоваться соответствующие сертифицированные по требованиям безопасности информации средства защиты.

6.6. Состав пользователей ЛВС устанавливается письменным приказом директора департамента здравоохранения и должен контролироваться. Все изменения состава пользователей, их прав и привилегий должны регистрироваться.

6.7. Каждый администратор и пользователь должен иметь уникальные идентификатор и пароль.

7. ЗАЩИТА ИНФОРМАЦИИ ПРИ МЕЖСЕТЕВОМ ВЗАИМОДЕЙСТВИИ

7.1. Контроль взаимодействия ЛВС с другими вычислительными сетями должен быть постоянным и осуществляться с использованием сертифицированных по требованиям безопасности информации средств контроля (средств обнаружения вторжений, мониторинга сети, активного аудита и т.д.). Коммуникационное оборудование и все точки соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах контролируемой зоны объекта информатизации.

7.2. При конфигурировании коммуникационного оборудования (маршрутизаторов, концентраторов, мостов и мультиплексоров) рекомендуется разделять трафик отдельных сетевых фрагментов с учетом решаемых задач пользователей ЛВС.

7.3. Подключение ЛВС к другой автоматизированной системе (локальной или распределительной вычислительной сети) должно осуществляться с использованием межсетевых экранов, требования к которым определяются документами ФСТЭК России (Гостехкомиссия).

Например, для защиты АС при ее взаимодействии с другой АС по каналам связи необходимо использовать:

- в АС класса 1Г – МЭ не ниже класса 4;
- в АС класса 1Д и 2Б, 3Б – МЭ класса 5 или выше.

8. ЗАЩИТА ИНФОРМАЦИИ ПРИ РАБОТЕ С СИСТЕМАМИ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

8.1. При работе с системами управления базами данных (СУБД) и базами данных (БД) необходимо учитывать следующие особенности защиты информации от НСД:

- в БД может накапливаться большой объем интегрированной информации по различным тематическим направлениям, предназначенной для различных пользователей;
- БД могут быть физически распределены по различным устройствам и узлам сети;
- БД могут включать различную конфиденциальную информацию;
- разграничение доступа пользователей к объектам БД (таблицам, схемам, процедурам, записям, полям записей в базах данных и т.п.), может осуществляться только средствами СУБД;
- регистрация действий пользователей при работе с объектами БД может осуществляться и средствами СУБД, если таковые имеются.

9. ВОЗМОЖНЫЕ ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ И НЕСАНКЦИОНИРОВАННОГО ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ И ПРОЦЕССЫ В УЧРЕЖДЕНИИ

9.1. Возможными каналами утечки речевой информации являются:

9.1.1. Акустическое излучение информативного речевого сигнала, которое может быть зарегистрировано путем непосредственного прослушивания акустических сигналов, а также в результате перехвата аппаратурой на основе направленных микрофонов.

9.1.2. Виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала за счет воздействия его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений, перехват которых может осуществляться контактными микрофонами-стетоскопами и оптико-электронной (лазерной) аппаратурой.

Для перехвата акустического сигнала с передачей информации по радиоканалу, ИК-каналу, ультразвуковому каналу, линиям связи и коммуникациям в технические средства и защищаемые помещения могут внедряться специальные электронные устройства перехвата информации («закладки»). Аппаратура сбора информации с указанных автоматических средств перехвата и управления ими может функционально объединяться с портативной и стационарной аппаратурой перехвата информации.

9.1.3. Электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации, выходящим за пределы контролируемой зоны.

9.1.4. Радиоизлучения, модулированные информативным речевым сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации технических средств.

9.1.5. Радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации.

9.1.6. Радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации («закладочные устройства»).

9.2. Возможными каналами утечки и воздействия на информацию и информационные ресурсы, представленные в виде носителей на магнитной и оптической основе, информативных электрических сигналов, информационных массивов и баз данных являются:

9.2.1. Побочные электромагнитные излучения информативного сигнала от технических средств и линий передачи информации.

9.2.2. Наводки информативного сигнала, обрабатываемого техническими средствами, на провода и линии, выходящие за пределы контролируемой зоны объектов департамента агропромышленного комплекса (на линии вспомогательных технических средств и систем, на цепи заземления и электропитания).

9.2.3. Изменения тока потребления, коррелированные с обрабатываемыми техническими средствами информативными сигналами.

9.2.4. Радиоизлучения, модулированные информативным сигналом, возникающие при наличии паразитной генерации в узлах (элементах) технических средств.

9.2.5. Радиоизлучения или электрические сигналы от внедренных в технические средства, подключенных к ним или каналам связи специальных электронных устройств перехвата информации («закладок»).

9.2.6. Съем информации путем контактного или индукционного подключения к кабельным линиям связи.

9.2.7.Перехват информации, передаваемой по радиоканалу.

9.2.8.Несанкционированный доступ к информации, обрабатываемой в автоматизированных системах.

9.2.9. Хищение технических средств и хранящейся в них информации или отдельных носителей информации.

9.2.10. Съем информации с аппаратных средств ЭВТ, автоматизированных систем при их передаче в другие организации, сдаче в ремонт и т.д.

9.2.11. Просмотр информации с экранов дисплеев и других средств ее отображения с помощью оптических средств.

9.2.12. Воздействие (физическое, дистанционное, электромагнитное и т.д.) на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена, в том числе через специально внедренные электронные и программные средства («закладки»).

10. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ

10.1. Общее руководство организацией работ по защите информации в Учреждении возлагается на Главного врача Учреждения. Для выполнения работ по защите информации могут привлекаться по договору организации, имеющие соответствующие лицензии ФСТЭК России (Гостехкомиссии) для проведения работ на даны вид деятельности.

Главный врач и заместитель директора, ответственный за организацию и руководство работами по защите информации, рассматривают предложения по совершенствованию системы защиты информации и принимают по ним обоснованные решения. Методическое руководство функционированием системы защиты информации в Учреждении осуществляется постоянно действующей технической комиссией по защите государственной тайны Тюменской области.

10.2. Непосредственная организация и разработка мероприятий по защите информации, а также по контролю эффективности принятых мер и используемых средств защиты возлагается на ответственного по защите информации.

10.3. Методическое руководство ответственного по защите информации Учреждения по вопросам защиты информации осуществляет подразделение по защите информации Главного управления специальных мероприятий Тюменской области и нештатный специалист по технической защите

информации управления по здравоохранению Администрации города Тюмени, департамента здравоохранения Тюменской области.

10.4. Организация и контроль выполнения мероприятий по защите информации при эксплуатации объектов информатизации сотрудниками Учреждения возлагается на главного врача Учреждения, в ведении которого находятся объекты информатизации, подлежащие защите. Данные функции главный врач осуществляет через подчиненных им специалистов по защите информации.

10.5. Работники, эксплуатирующие защищенный объект информатизации (пользователи автоматизированных систем и пр.), несут персональную ответственность за выполнением установленных правил и требований по обеспечению безопасности информации.

10.6. Практическая организация работ по защите информации в Учреждении, а также контролю эффективности принятых мер и используемых средств защиты, возлагается на ответственного по защите информации Учреждения. Основными его задачами являются:

• участие в анализе и выявлении возможных каналов утечки информации и воздействия на информационные ресурсы и процессы на объектах защиты;

• организация классификации автоматизированных систем от несанкционированного доступа к информации;

• организация выполнения организационно-технических мер защиты информации на объектах и аттестации объектов информатизации по требованиям безопасности информации;

• организация внедрения и эксплуатации средств защиты информации и систем информатизации и связи;

• контроль выполнения требований по защите информации и создания системы защиты информации в ходе строительства (реконструкции) объектов;

• разработка на базе руководящих и методических документов по защите информации в Учреждении организационно-распорядительных документов, определяющих порядок и мероприятия по защите информации на объектах;

• контроль выполнения требований по защите информации при эксплуатации объектов информатизации.

10.7. Ответственный по защите информации Учреждения выполняет обязанности администратора информационной безопасности, на которого возложено:

• руководство практическим выполнением работ по защите информации от

несанкционированных действий, разрушения и воздействия на нее при эксплуатации автоматизированных систем Учреждения;

• поддержание функционирования технических и программных средств и систем защиты информации, автоматизированных систем в установленных эксплуатационной документацией режимах;

• контроль технологического процесса обработки защищаемой информации и соблюдения требований инструкций при эксплуатации систем защиты информации пользователями автоматизированных систем;

• контроль целостности эксплуатируемого на средствах вычислительной техники программного обеспечения с целью выявления несанкционированных изменений в нем, а также выполнения мероприятий по антивирусной защите магнитных носителей информации и сообщений, получаемых по каналам связи;

• формирование и распределение реквизитов полномочий пользователей, определяемых эксплуатационной документацией на средства и системы защиты информации;

• разработка методических материалов по защите информации от несанкционированного доступа к ней, а также ее искажения и разрушения;

• обучение персонала и пользователей вычислительной техники правилам работы со средствами защиты информации;

• проведение служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации.

10.8. Все Учреждения участвуют в работах по защите информации, и взаимодействие их между собой с Департаментом здравоохранения Тюменской области и подразделением по защите информации ГУСМ области реализуется на административном и функциональном уровнях. Административный уровень определяет взаимодействие между подразделениями (специалистами) на основе требований постановлений и распоряжений руководства области на открытие работ по проведению определенного вида мероприятий по защите информации. Функциональный уровень - взаимодействие подразделений (специалистов) на основе их функций, определенных соответствующими положениями (функциональными обязанностями).

11. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

11.1. Контроль защиты информации - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях выявления и предотвращения утечки информации по техническим каналам; исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации; предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

11.2. Основными задачами контроля являются:

• проверка организации выполнения мероприятий по защите информации, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

• уточнение возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

• проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

• проверка выполнения требований по защите автоматизированных систем от несанкционированного доступа;

• проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

• проверка знаний работников по вопросам защиты информации и их соответствия необходимому уровню подготовки для конкретного рабочего места;

• оперативное принятие мер по пресечению нарушений требований (норм) защиты информации на объектах;

• разработка предложений по устранению (ослаблению) технических каналов утечки информации и воздействия на нее в деятельности объектов.

11.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей на объектах. Он осуществляется, как правило, по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации.

11.4. В ходе контроля проверяются:

• своевременность и полнота выполнения требований настоящего Положения и других руководящих документов по защите информации;

• полнота выявления возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

• эффективность применения организационных и технических мероприятий по защите информации;

• устранение ранее выявленных недостатков.

Кроме того, проводятся необходимые измерения и расчеты.

11.5. Основным видом технического контроля на объектах Учреждения является контроль эффективности защиты информации от утечки по техническим каналам, несанкционированного доступа к ней и программно-технических воздействий на информацию. Технический контроль выполнения норм и требований по защите информации по различным физическим полям проводится по соответствующим методикам ФСТЭК России (Гостехкомиссия).

11.6. Невыполнение предписанных мероприятий по защите конфиденциальной информации, считается предпосылкой к утечке сведений (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин не выполнения установленных требований по указанию главного врача или заместителя главного врача проводится служебное расследование.

Для проведения расследования назначается комиссия из компетентных лиц с привлечением ответственного за организацию работ по технической защите информации, ответственного по защите информации и работников подразделения, в котором произошло нарушение требований. В сложных случаях по согласованию привлекаются работники подразделения по защите информации ГУСМ области. Комиссия обязана установить, имела ли место утечка сведений конфиденциального характера и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования директором Учреждения принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

11.7. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов информатизации в Учреждении. Периодические, плановые и внезапные проверки объектов ЛПУ проводятся, как правило, силами подразделения по защите информации Департамента здравоохранения Тюменской области и Главным управлением специальных мероприятий Тюменской области (далее ГУСМ ТО) в соответствии с утвержденным планом или по предписаниям, подписанным руководителем области.

11.8. Одной из форм контроля защиты информации является обследование объектов информатизации и связи. Оно проводится рабочей группой в составе ответственного за организацию работ по технической защите информации, ответственного по защите информации и работников подразделения, в ведении которого находится объект информатизации.

11.9. Обследование объектов информатизации проводится с целью определения соответствия защищаемых помещений, основных и вспомогательных технических средств и систем требованиям по защите информации, установленным в «Аттестате соответствия».

11.10. В ходе обследования проверяется:

• соблюдение организационно-режимных требований и установленных требований по звукоизоляции защищаемых помещений;

• сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;

• наличие электробытовой, радио и телевизионной аппаратуры и устройств иностранного и непромышленного изготовления (пультов связи, устройств вызова и оповещения, усилителей, генераторов и других

вспомогательных технических средств и систем), которые могут способствовать возникновению каналов утечки информации;

• выполнение требований предписаний на эксплуатацию на основные технические средства и системы по их размещению относительно вспомогательных технических средств и систем, организации электропитания и заземления;

• соответствие выполняемых на объекте информатизации мероприятий по защите информации данным, изложенным в техническом паспорте;

• выполнение требований по защите автоматизированных систем от несанкционированного доступа;

• выполнение требований по антивирусной защите автоматизированных систем и средств вычислительной техники.

11.11. Для выявления радиоэлектронных устройств и проводов неизвестного назначения, преднамеренного нарушения защитных свойств оборудования, а также не предусмотренных правилами эксплуатации отводов от оборудования и соединительных линий, проложенных в защищаемых помещениях, а также других нарушений и способов возникновения каналов утечки информации необходимо:

• тщательно осмотреть мебель, сувениры (особенно иностранного производства), оборудование, установленное в этом помещении, осветительную аппаратуру, ниши отопительных батарей, шторы, оконные проемы и т.д.;

• вскрыть и осмотреть розетки, выключатели осветительной сети, люки вентиляции и каналы скрытой проводки;

• проверить качество установки стеклопакетов оконных приемов;

• провести аппаратурную проверку помещения на отсутствие возможно внедренных электронных устройств перехвата информации (при наличии соответствующей аппаратуры).

11.12. Кроме планового контроля, перед проведением в Учреждении мероприятий конфиденциального характера с использованием аппаратуры звукоусиления, ответственным по защите информации выполняются мероприятия технического контроля задействованных в мероприятиях помещений с целью выявления возможно внедренных в них электронных устройств перехвата информации, и проверка усилителей аппаратуры звукоусиления на самовозбуждение.

11.13. Контроль состояния защиты информации осуществляется при проверке ЛПУ департаментом здравоохранения или комиссией ГУСМ области.

11.14. Кроме того, проверка организации и состояния защиты информации на объектах ЛПУ может осуществляться ФСТЭК России и ФСБ РФ в соответствии с действующим законодательством Российской Федерации.

Доступ представителей указанных федеральных органов исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в

установленном порядке по предъявлении служебного удостоверения сотрудника, а также предписания установленной формы на право проведения проверки состояния защиты информации на данном объекте.

12. ПЛАНИРОВАНИЕ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ И КОНТРОЛЮ

12.1. Мероприятия по защите информации и по контролю выполнения требований руководящих и нормативно-методических документов по защите информации на объектах Учреждения, предусматриваются в Плане работы постоянно действующей технической комиссии Учреждения по защите государственной тайны, который утверждается главным врачом. При планировании мероприятий по контролю защиты информации отражаются: задачи контроля, перечень объектов, подлежащих контролю, сроки, ответственные исполнители, привлекаемые силы и средства контроля, порядок обобщения результатов контроля.

12.2. По результатам выполнения мероприятий по защите информации и контролю на объектах Учреждения готовится и представляется годовой отчет о мероприятиях по защите информации, отчет представляется в департаменте здравоохранения Тюменской области;

12.3. В отчете отражаются:

• перечень объектов защиты;

• перечень используемых сертифицированных средств защиты информации;

• анализ выполнения запланированных мероприятий по защите информации;

• результаты выполнения договоров со специализированными организациями в области обеспечения работ по защите информации в департаменте;

• результаты контроля защиты информации и в Учреждении, выявленные нарушения;

• проблемные вопросы обеспечения защиты информации и предложения по ее совершенствованию.

12.4. Контроль за выполнением работ по защите информации в Учреждении возлагается на директора или первого заместителя директора Учреждения.

13. АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

13.1. Объекты информатизации Учреждения, предназначенные для обработки информации, содержащей сведения конфиденциального характера, а также ведения конфиденциальных переговоров, подлежат обязательной аттестации по требованиям защиты информации.

Аттестация по требованиям безопасности информации предшествует началу обработки информации или ведения переговоров, и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте мер и средств защиты информации.

13.2. Аттестация объектов информатизации проводится при вводе объектов в эксплуатацию и в дальнейшем не реже, чем через три года, а также при изменении условий функционирования объектов информатизации, технологии обработки защищаемой информации и требований по безопасности информации. Аттестационные испытания осуществляются аттестационной комиссией, формируемой аккредитованным ФСТЭК России органом по аттестации из компетентных специалистов, в необходимых, для конкретного объекта информатизации, направлениях защиты информации, по согласованной соответственно с Учреждения программе испытаний.

13.3. При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от утечки по возможным физическим каналам и несанкционированного доступа к ней. Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта в реальных условиях эксплуатации с целью оценки

соответствия использованного комплекса мер и средств защиты требуемому уровню безопасности информации.

13.4. При проведении аттестационных испытаний применяются следующие методы проверок и испытаний:

- экспертно-документальный метод;
- инструментальный метод;
- расчетный метод;
- расчетно-инструментальный метод;
- попытка «взлома» систем защиты информации.

13.5. Для проведения испытаний подразделение Учреждения, ответственное за эксплуатацию аттестуемого объекта информатизации совместно с ответственным по защите информации представляет аттестационной комиссии следующие исходные данные и документацию:

- техническое задание на объект информатизации;
- технический паспорт на объект информатизации;
- приемо-сдаточную документацию на объект информатизации;
- акты категорирования защищаемых помещений и технических средств и систем;
- акт классификации АС по требованиям защиты информации;
- состав технических и программных средств, входящих в АС (или технических средств, расположенных в защищаемом помещении);
- планы размещения основных и вспомогательных технических средств и систем;
- состав и схемы размещения средств защиты информации;

• план контролируемой зоны;

• схемы прокладки линий передачи данных;

• схемы и характеристики систем электропитания и заземления объекта информатизации;

• перечень защищаемых в АС ресурсов с документальным подтверждением степени конфиденциальности каждого ресурса или конфиденциальности обсуждаемых в защищаемом помещении вопросов;

• организационно-распорядительная документация разрешительной системы доступа персонала к защищаемым ресурсам АС (обсуждаемым вопросам);

• описание технологического процесса обработки информации в АС;

• технологические инструкции пользователям АС и администратора безопасности информации.

• инструкции по эксплуатации средств защиты информации;

• предписания на эксплуатацию технических средств и систем;

• протоколы специальных исследований технических средств и систем;

• акты или заключения о специальной проверке защищаемых помещений и технических средств;

• сертификаты соответствия требованиям по безопасности информации на средства и системы обработки и передачи информации, используемые средства защиты информации;

• данные по уровню подготовки кадров, обеспечивающих защиту информации;

• данные о техническом обеспечении средствами контроля эффективности защиты информации и их метрологической поверке;

• нормативную и методическую документацию по защите информации и контролю эффективности защиты

Приведенный общий перечень исходных данных и документации может уточняться в зависимости от особенностей аттестуемого объекта информатизации по согласованию с аттестационной комиссией.

13.6. По результатам аттестационных испытаний оформляется «Заключение…», которое доводится до заявителя. На основании «Заключения…» принимается решение о выдаче специального документа - «Аттестата соответствия», подтверждающего, что объект соответствует требованиям стандартов или иных нормативных документов по защите информации, утвержденных ФСТЭК России, или другими органами государственного управления в пределах их компетенции.

13.7. На основании выданного специализированной организацией аттестата соответствия главный врач, издает приказ о разрешении обработки конфиденциальной информации на объекте информатизации и назначении лиц ответственных за обеспечение защиты информации при его эксплуатации.

14. ВЗАИМОДЕЙСТВИЕ С УЧРЕЖДЕНИЯМИ И ОРГАНИЗАЦИЯМИ ПО ВОПРОСАМ ЗАЩИТЫ ИНФОРМАЦИИ

14.1. Основной структурой, с которой взаимодействуют Учреждение по вопросам защиты информации, является подразделение по защите информации Главного управления специальных мероприятий Тюменской области.

Основными направлениями взаимодействия являются:

- координация мероприятий по защите объектов информатизации;
- разработка организационно-распорядительных документов по организации работ по защите информации в Учреждении;
- организация взаимодействия с организациями, представляющими услуги по защите информации;
- консультация специалистов Учреждения, подведомственных организаций, выдача рекомендаций, осуществление контроля состояния работ по защите информации от утечки по техническим каналам;
- рассмотрение проектов организационно-технических документов по защите объектов информатизации, разработанных в структурных подразделениях Учреждения, и проектов договоров Учреждения со сторонними организациями по обеспечению защиты информации на объектах Учреждения;
- финансирование работ в Учреждении по защите информации;
- предоставление и анализ отчетных документов Учреждения, по обеспечению защиты информации.

14.2. Учреждение взаимодействует со сторонними организациями, имеющими лицензии ФСТЭК России или ФСБ РФ на деятельность в области защиты информации. Каждая из таких организаций привлекается к работам по защите информации в интересах Учреждения в рамках договоров в соответствии с перечнем услуг, представляемых этой организацией, указанных в лицензии (к услугам относится и продажа средств защиты информации и поисковых приборов). Выбор организации на проведение работ в области защиты информации на объектах Учреждения производится в соответствии с установленным порядком, и предпочтение отдается организациям:

- имеющим лицензии по всему комплексу работ в области защиты информации, которые необходимо проводить на объектах Учреждения;
- имеющим в качестве учредителей федеральные органы и государственные предприятия;
- имеющим штат сотрудников, позволяющий проводить работы по всем направлениям деятельности в полном объеме;
- ранее выполнявшим работы для Учреждения и положительно себя рекомендовавшим.

Со сторонней организацией могут заключаться и договоры на выполнение защиты объекта (объектов) информатизации «под ключ». В этом случае указанная организация проводит все работы по защите информации,

получая от Учреждения все исходные данные и согласовывая проектные, технические и программные проработки с ответственным по защите информации, подведомственными организациями.

14.3. Запрещается привлекать для проведения работ по защите информации на объектах иностранные организации, а также размещать на территории указанных объектов совместные с иностранными государствами предприятия.

При подготовке решения о сдаче в аренду части территории объекта в пределах контролируемой зоны ответственным по защите информации проводится дополнительная оценка достаточности внедренного комплекса мер защиты информации на объектах информатизации. Сформированные требования к предполагаемому арендатору, обусловленные решением задач по технической защите Учреждения, включаются в договор аренды.

14.4. При организации взаимодействия Учреждения с другими учреждениями и органами, по вопросам основной деятельности, меры по защите информации, представляющей интерес для Учреждения, принимаются в зависимости от обстоятельств отдельным согласованным решением.