**«УТВЕРЖДАЮ»**
Директор
бюджетного учреждения
Ханты-Мансийского автономного
округа – Югры «Медицинский
информационно-аналитический центр»

_____ В.М.Нусинов

«_18_» ___02___ 2015 год

# Стратегия информационной безопасности медицинских организаций Ханты-Мансийского автономного округа – Югры

Стратегию разработал
Начальник отдела по защите информации _____ «_18_» ___02___ 2015 г. Устинов Д.В
(Должность) ( Подпись) (Фамилия .И.О)

# ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

| Сокращение | Определение |
|---|---|
| СУБД | Система управления базами данных |
| ПДн | Персональные данные |
| ИСПДн | Информационная система персональных данных |
| ИС | Информационная система |
| ИР | Информационный ресурс |
| ИБ | Информационная безопасность |
| НСД | Несанкционированный доступ |
| ФСТЭК России | Федеральная служба технического и экспортного контроля |
| ФСБ России | Федеральная служба безопасности России |
| СЗИ | Средства защиты информации |
| СКЗИ | Средства криптографической защиты информации |
| ПО | Программное обеспечение |
| МО | Медицинская организация |
| ТС | Техническое средство |
| СОИБ | Система обеспечения информационной безопасности |
| КСИИ | Ключевая система информационной инфраструктуры |
| ИАС | Идентификация и аутентификации субъектов |
| ЗПИ | Защита потоков информации |
| РАС | Регистрация и аудит событий |
| УИБ | Управление информационной безопасностью |
| КДС | Контроль и управления доступом субъектов |
| ПДС | Поддержки доверенной среды |
| СУИБ | Система управления ИБ |

# ВВЕДЕНИЕ

Стратегия информационной безопасности медицинских организаций Ханты-Мансийского автономного округа – Югры - (далее Стратегия) является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности в медицинских организациях Ханты-Мансийского автономного округа – Югры, при оказании государственных услуг юридическим и физическим лицам, информационного обмена между медицинскими организациями Ханты-Мансийского автономного округа – Югры, а так же информационного взаимодействия с федеральными, региональными и муниципальными органами власти.

Стратегия не является техническим проектом системы защиты информации, а определяет пути достижения требуемого уровня защищенности информации (обеспечения её целостности, доступности и конфиденциальности) при повседневной деятельности медицинских организаций Ханты – Мансийского автономного округа – Югры в ходе оказания государственных информационных услуг через создание продуманной, многокаскадной системы обеспечения информационной безопасности. СОИБ должна строиться на основе комплексирования разнообразных организационных и технических мер защиты, опираться на современные методы прогнозирования, анализа и моделирования возможных угроз безопасности информации и снижения (ликвидацию) ущерба от их воздействия.

Стратегия является верхнеуровневым документом отражающим официально принятую бюджетным учреждением Ханты-Мансийского автономного округа-Югры «Медицинский информационно-аналитический центр» систему взглядов на обеспечение информационной безопасности в учреждениях и пути её решения. Другими верхнеуровневыми документами являются Политика обеспечения безопасности МО, Политика обеспечения безопасности БУ «Медицинский информационно-аналитический центр» и Концепция безопасности БУ «Медицинский информационно-аналитический центр». Все эти документы наряду с локальными политиками, инструкциями, регламентами, журналами, положениями составляют иерархическую систему документов по обеспечению ИБ.

Нормативные и организационно-распорядительные документы подведомственных учреждений Департамента здравоохранения Ханты-Мансийского автономного округа – Югры (далее - Департамент), затрагивающие вопросы ИБ, должны разрабатываться с учетом положений настоящей Стратегии и не противоречить им.

### 1.1. Сфера применения Стратегии

Положения Стратегии предназначены для использования в практической деятельности должностных лиц, ответственных за создание и использование информационных систем МО и развитие телекоммуникационной инфраструктуры, по обеспечению требуемого уровня защищенности, а также участников информационного взаимодействия, по соблюдению ими установленных требований безопасности информации.

Положения Стратегии могут быть использованы для обеспечения защиты информации, полученной от субъектов персональных данных (физических лиц), органов государственной власти и прочих организаций. Дополнительные или взаимно оговоренные сторонами требования по защите не могут ослаблять уровень ИБ информационной системы МО.

Стратегия должна способствовать установлению единой технической политики в сфере обеспечения ИБ и созданию необходимых условий для соответствующих эффективных действий подразделений медицинских организаций. Стратегия является методологической основой:

- при формировании единой политики обеспечения ИБ в Департаменте и подведомственных учреждениях;
- при разработке и совершенствовании документов методического и организационного обеспечения безопасности информации;
- при выработке лицами, ответственными за реализацию политики ИБ, взаимосвязанных и согласованных мер защиты организационного и технического характера;
- при разработке уполномоченными лицами МО и проектными организациями предложений по созданию и развитию ИС медицинских организаций и телекоммуникационной инфраструктуры;
- при принятии должностными лицами Департамента здравоохранения управленческих решений по реализации выработанной политики обеспечения ИБ;
- при определении ролей и ответственности должностных лиц и работников Департамента здравоохранения в сфере обеспечения безопасности информации;
- при координации деятельности медицинских организациях, учреждений и организаций, подведомственных Департаменту Здравоохранения, по созданию, развитию и эксплуатации ИС медицинских учреждений Ханты - Мансийского автономного округа - Югры;
- при разработке замысла защиты информации в ИС медицинских организаций, Стратегии облика СЗИ ИС в соответствии с ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения», и ГОСТ Р 53114-2008. «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения», стандартами ГОСТ Р ИСО МЭК серий 13325, 15408, 17779, 27003, 27005, нормативными документам ФСТЭК России и ФСБ России, Роскомнадзора и других регулирующих органов,
- при разработке технических заданий на создание (модернизацию) объектов информатизации медицинских организаций.

Требования по защите информации и проектированию защищённых ИС конкретизируются в других документах, Политики ИБ с указанием комплекса мер и средств, направленных на выявление, предотвращение и противодействие различным угрозам безопасности информации.

### 1.2. Правовая основа обеспечения ИБ

Правовой основой обеспечения ИБ являются положения Конституции Российской Федерации, федеральных законов, указов Президента Российской Федерации, постановлений и распоряжений Правительства Российской Федерации, нормативных правовых актов законодательства Российской Федерации, нормативных и руководящих документов ФСТЭК России и ФСБ России по вопросам защиты информации.

При реализации функций оказания государственных услуг в системе здравоохранения обрабатывается информация, содержащая сведения, составляющие:

- служебную информацию Департамента и других органов государственной власти;
- врачебную тайну;
- персональные данные;
- сведения, на основании которых принимаются управленческие решения, отнесенные к сведениям КСИИ;
- открытые данные, подмена, искажение или уничтожение которых может нанести ущерб интересам отдельных граждан, организаций, обществу и государству в целом.

Базовым законом в области обеспечения ИБ является Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» устанавливающий необходимость защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

Основу правового обеспечения деятельности Департамента устанавливает Федеральный закон от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации", вводящий понятие врачебной тайны, (ст.13 данного закона).

Особое место в правовой основе обеспечения ИБ занимает Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

### 1.3. Цели обеспечения безопасности информации

Главной целью обеспечения безопасности информации является предотвращение (минимизация) ущерба субъектам правоотношений в результате противоправных действий с информацией, приводящих к ее разглашению, утрате, утечке, искажению (модификации), уничтожению или незаконному использованию, либо нарушению работы ИС медицинских организаций и телекоммуникационной инфраструктуры, используемой для информационного обмена и взаимодействия с органами государственной власти и медицинскими организациями.

Основными целями обеспечения безопасности информации являются:

- предотвращение несанкционированного доступа к информации;
- предотвращение нарушений прав субъектов при обработке информации;
- предупреждение последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации;
- недопущение деструктивного информационного воздействия на информацию.

### 1.4. Основные задачи обеспечения безопасности информации

Основными задачами, вытекающими из целей обеспечения безопасности информации, являются:

- совершенствование политики в области ИБ при создании и внедрении ИС медицинских организаций и телекоммуникационной инфраструктуры;
- обеспечение соответствия мер и средств защиты информации в ИС медицинских организаций положениям нормативных документов по безопасности информации;
- совершенствование нормативно-правовой базы обеспечения ИБ, координация деятельности медицинских организаций по защите информации;
- обеспечение полноты, достоверности и оперативности получения информации органами государственной власти, а также информационной поддержки принятия управленческих решений аппаратом Департамента здравоохранения;
- защита от вмешательства в процесс функционирования ИС медицинских организаций посторонних лиц, совершенствование СЗИ, ее организации, форм и методов предотвращения и нейтрализации угроз ИБ, ликвидации последствий;
- предотвращение, в том числе с использованием организационно-правовых мер и технических средств защиты информации, несанкционированных действий и незаконных посягательств на информационные ресурсы со стороны посторонних лиц и работников медицинских организаций;
- регистрация событий, влияющих на безопасность информации, обеспечение полной подконтрольности и подотчетности выполнения всех операций, совершаемых в ИС медицинских организаций;
- своевременное выявление, оценка и прогнозирование источников угроз, причин и условий, способствующих нанесению ущерба интересам субъектов, нарушению нормального функционирования и развития ИС медицинских организаций и телекоммуникационной инфраструктуры;
- анализ рисков реализации угроз, оценка возможного ущерба, предотвращение в медицинских организациях последствий нарушения ИБ, создание условий для минимизации, локализации и максимально возможного возмещения ущерба;
- обеспечение возможности восстановления актуального состояния ИС медицинских организаций и телекоммуникационной инфраструктуры при нарушении ИБ;
- создание СУИБ.

### 1.5. Ответственность за реализацию положений Стратегии

За реализацию положений Стратегии отвечают лица, входящие в организационную структуру системы обеспечения безопасности информации, в том числе (но не ограничиваясь):

- структурные подразделения Департамента;
- подведомственные учреждения (МО) Департамента;
- разработчики ИС и объектов информатизации Департамента.

## II. ОБЪЕКТЫ ЗАЩИТЫ

### 2.1. Информация, как объект права

В соответствии со статьями 5, 6 Федерального закона Российской Федерации «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27 июля 2006 г.

Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Обладатель информации (физическое лицо, юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование), если иное не предусмотрено федеральными законами, может:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать свои права способами, установленными законом, в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации при осуществлении своих прав обязан:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

### 2.2. Информация, как объект защиты

БУ «Медицинский информационно-аналитический центр» обеспечивает в пределах своей компетенции защиту сведений, составляющие охраняемые законом сведения, а также контроль и координацию деятельности по защите таких сведений в МО Ханты – Мансийского автономного округа - Югры.

Информация, содержащаяся в информационных ресурсах, а также иные имеющиеся в распоряжении сведения и документы формирующихся в процессе деятельности МО. Часть из них может быть отнесена к общедоступной информации, а часть - к информации ограниченного доступа, в том числе составляющей врачебную, служебную, коммерческую

тайну, ПДн. Часть открытых ИР содержит сведения, неправомерное обращение с которыми может нанести ущерб гражданам, организациям, обществу.

Защита ИР, содержащих информацию ограниченного доступа (распространения), представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации;
- реализацию права на доступ к информации в соответствии с законодательством Российской Федерации;

***2.2.1 ИР, содержащие общедоступную (публичную) информацию (далее - Открытые ИР).***

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не может быть ограничен, а именно к:

- нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления, а так же другими нормативно-правовыми актами МО обязательных для общего доступа;
- информации о состоянии окружающей среды;
- информации о деятельности медицинской организации, а также об использовании бюджетных средств (за исключением сведений, составляющих информацию ограниченного доступа (распространения);
- информации, накапливаемой в государственных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией (сайты медицинских организаций);
- информации, расположенной на официальном сайте МО;
- информации, являющейся общедоступными ПДн, обрабатываемых в МО;
- иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

на:

- обеспечение защиты информации от уничтожения, модифицирования, блокирования, а также от иных неправомерных действий в отношении такой информации;
- реализацию права каждого на доступ к информации.

***2.2.2. ИР, содержащие информацию ограниченного доступа (распространения)***

К ИР медицинских организаций, содержащим информацию ограниченного доступа (распространения), относятся информация конфиденциального характера:

- Медицинские ИР – ресурсы содержащие полученные медицинскими организациями сведения о пациентах (врачебная тайна);
- ИР персональных данных - ресурсы, содержащие сведения, составляющие персональные данные работников медицинских организаций (ресурсы: «Бухгалтерия», «Кадры» и другие);

- Служебные ИР - ресурсы, содержащие агрегированные сведения, необходимые для обеспечения работы информационно-аналитической системы медицинской организации;
- Технологические ИР - ресурсы, содержащие сведения о принципах, методах, технических решениях и правилах обеспечения безопасности информации в Департаменте и медицинских организациях.

### 2.3. Элементы инфраструктуры, как объекты защиты

Информация не может быть рассмотрена в отрыве от элементов инфраструктуры медицинских организаций (объекта информатизации), на которых она обрабатывается (хранится, обсуждается), поэтому областью действий по защите ИР является инфраструктура ИС медицинских организаций, в том числе:

- помещения, здания, объекты, сооружения, передвижные объекты медицинских организаций, предназначенные для работы с информацией;
- оборудование ИС (серверные комплексы, рабочие станции пользователей, технические средства ввода/вывода информации, комплексы сканирования документов, принтеры, средства хранения и архивирования данных, источники бесперебойного питания);
- телекоммуникационные сети и системы (активное и пассивное коммуникационное оборудование, система управления, мониторинга и обслуживания инфраструктурой);
- средства и системы связи и передачи данных (ведомственной, междугородней, городской, внутренней);
- программные средства (операционные системы, системы управления базами данных, другое общесистемное, специальное и прикладное программное обеспечение);
- средства защиты информации;
- технические средства приема, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации);
- средства обеспечения жизнедеятельности объектов (гарантированные и бесперебойные системы электропитания и заземления объектов, системы пожарной и охранной сигнализации, электронные системы контроля и управления доступом на территорию и в помещения, системы громкоговорящей связи и оповещения, системы кондиционирования, отопления, вентиляции и пожаротушения).

Информация может быть представлена в виде электронных сообщений (электронных документов), формируемых в ходе информационного взаимодействия с государственными органами, исполнения медицинскими организациями своих функций по оказанию государственных услуг. Используемые при этом технологии информационного взаимодействия должны обеспечивать требуемый уровень защиты ИР при использовании:

- обмена электронными сообщениями между медицинскими организациями и взаимодействующими структурами;
- обмена электронными файлами в рамках электронного документооборота, с применением электронной подписи;
- обмена файлами между медицинскими организациями и взаимодействующими государственными органами на машинных носителях;

- Web-доступа пациентов при получении государственных услуг с использованием ИР медицинских организаций;
- технологий терминального доступа работников медицинских организаций
- Информация может быть представлена на различных материальных носителях, к которым относятся:
- бумажные носители информации (документы);
- машинные носители информации (магнитные, магнитооптические, оптические, flash-накопители, карты памяти различных типов и др.);
- информация может распространяться в виде информативных сигналов (электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта информация, обрабатываемая в ИС).

ИС Департамента относится к ключевым системам информационной инфраструктуры, которая осуществляет контроль за процессами медицинского обслуживания граждан. В результате деструктивных информационных воздействий на ИС медицинских организаций может сложиться чрезвычайная ситуация или будут нарушены выполняемые Департаментом функции управления со значительными негативными социальными последствиями.

## III. РЕЖИМ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

### 3.1. Обобщенная структура информационных ресурсов

В ИС медицинских организациях могут одновременно использоваться (обрабатываться) ИР различных обладателей информации, по отношению к которым установлены различные требования по степени ограничения доступа (распространения). При этом ИР, отнесенные к одной категории доступа, могут иметь различные степени ограничения доступа.

### 3.2. Права по установлению требований по защите информационных ресурсов

В зависимости от принадлежности ИР и характера, содержащейся в них информации, Департамент здравоохранения имеет право установить требования по обеспечению ИБ (режим защиты).

Безопасность информации, содержащей государственную тайну, организуют регуляторы, которые определяют степень защиты и выдвигают требования, обязательные к исполнению всеми организациями на территории Российской Федерации. Такими органами являются:

- Межведомственная комиссия (МВК) по защите государственной тайны (в части координации деятельности);
- ФСБ России (в части допуска к работам со сведениями, содержащими государственную тайну, и применения криптографических (шифровальных) средств защиты информации);
- ФСТЭК России (в части защиты не криптографическими методами).

Требования по защите информации, содержащейся в государственных ИС, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности (ФСБ России) и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты

информации (ФСТЭК России), в пределах их полномочий. При создании и эксплуатации государственных ИС, используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

Требования по обеспечению ИБ (режим защиты) открытых (общедоступных) ИР, определяются медицинскими организациями, как их обладателем, самостоятельно на основе требований, определяемых регуляторами, которые в этом случае носят рекомендательный характер. Департамент здравоохранения, как обладатель сведений на законных основаниях, имеет право предъявлять требования по обеспечению режима защиты, принадлежащей ему информации, и требовать его соблюдения при передаче такой информации в другие органы государственной власти и третьим лицам. Такие требования носят обязательный характер для всех пользователей.

При обработке персональных данных медицинские организации обязаны принимать необходимые организационные и технические меры для защиты персональных данных (режим защиты), которые предусмотрены, Федеральным законом № 152-ФЗ от 27.07.2006 г. «О персональных данных», постановлениями Правительства Российской Федерации и нормативно-методическими документами регуляторов в области защиты персональных данных и информации.

### 3.3. Порядок установления режима защиты ИР

Режим защиты в отношении ИР ограниченного доступа, не содержащих сведения, отнесенные к государственной тайне, считается установленным после принятия медицинской организацией следующих мер:

- утверждения Политики информационной безопасности, в том числе политики оператора в отношении обработки ПДн;
- утверждения перечня информации, подлежащей защите;
- ограничения доступа к защищаемым ИР, в том числе обращающимся в ИС медицинской организации;
- установления порядка обращения с ИР, в том числе другими субъектами;
- организации контроля за соблюдением порядка обращения к защищаемым ИР;
- организации учета лиц, получивших доступ к защищаемым ИР и (или) лиц, которым защищаемая информация была предоставлена;
- урегулирования отношений по использованию защищаемых ИР с работниками (трудовые договоры) и другими субъектами (гражданско-правовые договоры);

## IV. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И БАЗОВАЯ МОДЕЛЬ НАРУШИТЕЛЯ

### 4.1. Базовая модель угроз безопасности информации

#### *4.1.1. Область применения Базовой модели угроз безопасности информации*

Базовая модель угроз содержит единые исходные данные по актуальным для объектов МО угрозам безопасности информации, связанным с несанкционированным, в том числе случайным, доступом с целью ознакомления, изменения, копирования, неправомерного распространения информации или деструктивных воздействий на элементы ИС и обрабатываемой в них информации. Базовая модель предназначена для формирования обоснованных требований по обеспечению безопасности информации.

Базовая модель угроз представляет собой систематизированный перечень основных актуальных угроз, их источников, уровней реализации угроз, типов материальных объектов среды обработки информации, актуальных для объектов информатизации МО.

Для отдельных объектов должны быть разработаны Частные модели актуальных угроз, учитывающие особенности обработки информации на конкретном объекте. В качестве методологии выбора актуальных угроз и составления Частных моделей угроз может использоваться общая методология и положения настоящего раздела Стратегии.

### *4.1.2. Общий подход к моделированию угроз безопасности информации*

Под угрозами безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реальную опасность утечки защищаемой информации, несанкционированных и (или) непреднамеренных воздействий на неё. Систематизация угроз в Базовой модели проведена по виду нарушаемого свойства безопасности информации:

1) угрозы нарушения конфиденциальности:

- хищение (утечка, перехват, съем) информации и средств ее обработки;
- утрата (неумышленная потеря) информации, средств ее обработки;
- разглашение информации;

2) угрозы нарушения целостности информации:

- модификация (искажение) информации;
- отрицание подлинности информации;
- навязывание ложной информации;
- не подтверждения получения информации;

3) угрозы нарушения доступности информации:

- блокирование информации;
- отказ работы пользователей;
- отказ (ошибки) средств обработки и хранения информации;
- уничтожение информации и средств её обработки и хранения;

Моделирование процессов нарушения безопасности информации осуществляется применительно к объекту информатизации на основе рассмотрения логической цепочки взаимодействия при реализации угрозы:

«угроза - источник угрозы - уровень реализации - уязвимость - последствия».

В качестве источников угроз могут выступать как субъекты (физические лица, организации), так и случайные явления (стихийные бедствия, сбои в ПО, отказ инженерных систем и т.д.). Источники угроз могут находиться как внутри объекта информатизации - внутренние, так и вне его - внешние. Все источники угроз делятся на классы, обусловленные типом носителя угрозы (источника угрозы):

- антропогенные источники угроз, обусловленные действиями субъекта, которые могут быть квалифицированы как умышленные или случайные проступки;
- техногенные источники угроз, обусловленные техническими средствами и определяемые технократической деятельностью человека;

– стихийные источники угроз, обусловленные природными явлениями, которые невозможно предусмотреть или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей.

### *4.1.3. Актуальные источники угроз и уязвимости объектов медицинских организаций*

Для объектов информатизации медицинских организаций основными актуальными источниками угроз безопасности информации для всех или части ИР являются:

– компьютерные злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том числе с использованием компьютерных вирусов и других типов вредоносных кодов (антропогенные, внешние);
– поставщики программно-технических средств, расходных материалов, услуг, в том числе провайдеры телематических услуг (антропогенные, внешние);
– подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования ИС медицинских организаций и его ремонт (антропогенные, внешние);
– работники медицинских организаций, являющиеся легальными участниками процессов обработки информации и действующие вне рамок предоставленных полномочий (антропогенные, внутренние);
– работники медицинских организаций, являющиеся легальными участниками процессов обработки информации и действующие в рамках предоставленных полномочий (антропогенные, внутренние);
– неблагоприятные события природного характера, в том числе пожары, стихийные бедствия, магнитные бури, природные катаклизмы (стихийные);
– неблагоприятные события техногенного характера, в том числе аварии на средствах инженерных коммуникаций, средствах телекоммуникационной инфраструктуры, сбои и отказы оборудования (техногенные).

Для объектов медицинских организаций актуальными уязвимостями являются:

– ошибки в проектировании объектов информатизации МО и телекоммуникационной инфраструктуры, влияющие на их отказоустойчивость и катастрофоустойчивость, в том числе сбои электроснабжения, физический износ оборудования и сооружений, малое время наработки на отказ оборудования и ПО;
– физические, моральные, психологические особенности работников, создающие предпосылки террористического или криминального воздействия, в том числе: антагонистические отношения (зависть, озлобленность, обида), неудовлетворенность своим положением, неудовлетворенность действиями руководства (взыскание, увольнение), психологическая несовместимость, психические отклонения, стрессовые ситуации, физическое состояние субъекта (усталость, болезненное состояние), психосоматическое состояние субъекта;
– недостатки в организации охраны и технической укрепленности объектов медицинских организаций, в том числе нарушения режима охраны и защиты (доступа на объект, доступа к техническим средствам), нарушения режима эксплуатации технических средств (энергообеспечения, жизнеобеспечения);
– восприимчивость ПО к вредоносным программным кодам и компьютерным вирусам;
– наличие уязвимостей программного и аппаратного обеспечения, в том числе оставление разработчиком (умышленное или случайное) возможностей несанкционированной модификации программного кода, использования среды программирования ИС, программных вызовов;
– сбои и отказы технических средств, ошибки при подготовке и использовании ПО;
– наличие уязвимостей (слабостей) системы защиты информации;

- несоответствующая утвержденной документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения, некомпетентные действия работников при конфигурировании и управлении программными средствами и оборудованием;
- некачественная (неполная) регламентация в договорах (контактах) вопросов взаимодействия с поставщиками и подрядчиками (обязанности, ответственность);
- несоответствие регламентов деятельности текущему состоянию объекта защиты и неконтролируемость исполнения работниками МО регламентов своей деятельности, в том числе инсталляции нештатного ПО, нарушения порядка обработки и обмена информацией, хранения и уничтожения носителей информации.

### 4.2. Базовая модель нарушителя безопасности информации

Все нарушители делятся на две основные группы: внутренние и внешние.

Под внутренними потенциальными нарушителями подразумеваются работники медицинских организаций, имеющие санкционированный доступ на территорию медицинских организаций или к ИР.

Под внешними потенциальными нарушителями подразумеваются все остальные лица.

Перечень потенциальных нарушителей безопасности, который включает внешних и внутренних нарушителей определен регуляторами. В данном разделе рассматриваются особенности, которые могут влиять на ИБ МО.

Рассматриваемые настоящей Стратегией вопросы ИБ в КСИИ предусматривают в случае необходимости, возможность создания частных моделей угроз и нарушителя безопасности информации для объектов КСИИ.

Применительно к безопасности персональных данных следует руководствоваться Моделью угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных медицинской организации.

В соответствии с принципами классификации нарушителей, установленной ФСБ России, и с учетом предположений об имеющихся у них возможностях, нарушители телекоммуникационной инфраструктуры относятся к следующим типам:

| № п/п | Вид нарушителя | Тип нарушителя |
|---|---|---|
| 1. | Внешние нарушители | |
| 1.1 | Внешний нарушитель, не имеющий прав доступа в контролируемую зону | * |
| 1.2 | Сотрудник сторонней организации, не являющийся зарегистрированным пользователем ИС медицинской организации, но имеющий право доступа в контролируемую зону | * |
| 1.3 | Внешний нарушитель, не являющейся сотрудником сторонней организации, но не имеющей право доступа в контролируемую зону | |
| 2. | Внутренние нарушители | |
| 2.1 | Работник медицинской организации, не являющийся зарегистрированным пользователем ИС медицинской организации, но имеющий право доступа в контролируемую зону | * |
| 2.2 | Работник медицинской организации, являющийся зарегистрированным | |

| | | |
|---|---|---|
| | пользователем ИС медицинской организации, но не имеющий администраторских прав | |
| 2.3 | Работник медицинской организации, являющийся зарегистрированным пользователем ИС медицинской организации, и имеющий администраторские права. | |

Анализ предположений о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности, в соответствии с действующей классификацией, нарушители безопасности телекоммуникационной инфраструктуры медицинских организаций более всего приближены к типу *. Этот тип нарушителя определяется как, самостоятельно осуществляющий создание методов и средств реализации атак, а также самостоятельно реализующий атаки.

При рассмотрении модели угроз безопасности информации и нарушителя информационной безопасности МО, в данной Стратегии не рассматривается возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков подсистем ИС, а так же сговора внутреннего и внешнего нарушителей, в связи с применением организационно-технических и кадрово-режимных мер.

При рассмотрении моделей угроз и нарушителя ИБ медицинских организаций, предполагается, что нарушитель знаком с требованиями безопасности информации (за исключением специальных требований СКЗИ) и является квалифицированным специалистом в области информатизации.

### 4.3. Возможный ущерб от нарушения безопасности информации

В ходе разработки, внедрения, эксплуатации и совершенствования объектов информатизации медицинских организаций, субъектам правоотношений, могут быть причинены следующие виды ущерба (вреда):

- материальный (экономический) ущерб любому субъекту от разглашения информации, являющейся объектом защиты;
- моральный вред, материальный ущерб любому субъекту персональных данных, от их разглашения или нарушения конституционных прав и свобод граждан;
- материальный ущерб от необходимости восстановления любым субъектом нарушенных прав и объектов защиты;
- моральный вред, материальный ущерб от дезорганизации деятельности МО;
- материальный ущерб МО от уничтожения (утраты) объектов защиты;
- материальный ущерб, моральный вред от несвоевременного поступления информации потребителям государственных информационных услуг или от нарушения целостности предоставленной информации;
- материальный ущерб от невозможности выполнения МО обязательств перед третьей стороной.

Система обеспечения ИБ медицинской организации должна обеспечить минимизацию возможного ущерба для субъектов правоотношений, участвующих в информационном обмене и использующих ИР медицинских организаций.

### 4.4. Основные методы противодействия угрозам безопасности информации

Вероятность реализации угроз уменьшается различными методами, направленными с одной стороны на устранение носителей угроз - источников угроз, а с другой на устранение или существенное ослабление основ их реализации - уязвимостей. Кроме того, эти методы должны быть направлены на устранение последствий реализации угроз. Среди методов противодействия выделяются следующие основные группы:

- правовые методы;
- экономические методы;
- организационные методы;
- инженерно-технические методы;
- технические методы;
- программно-аппаратные методы.

## V. ОРГАНИЗАЦИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

### 5.1. Направления сохранения свойств информации для достижения цели обеспечения безопасности информации

#### *5.1.1. Взаимосвязь направлений сохранения свойств информации и угроз ИБ*

Главная цель обеспечения ИБ достигается сохранением совокупности свойств информации, к основным из которых относятся:

- конфиденциальность защищаемых ИР;
- целостность защищаемых ИР;
- доступность ИР.

В зависимости от выбранного направления сохранения свойств информации, формируется состав требований к средствам защиты и организационным мероприятиям по ликвидации возможных угроз. Направления сохранения свойств информации могут иметь разную степень приоритета для разных ИР медицинской организации. Наличие приоритета по одному или нескольким направлениям не исключает необходимости обеспечения безопасности информации по другим направлениям сохранения свойств информации.

#### *5.1.2. Сводные сведения по приоритетным направлениям сохранения свойств информации*

При использовании ИР, приоритетными направлениями сохранения свойств информации при обеспечении ИБ являются:

| **Информационные ресурсы медицинской организации** | **Приоритеты направлений сохранения свойств информации:** | | |
|---|---|---|---|
| | **Конфиденциальность** | **Целостность** | **Доступность** |
| Конфиденциальные информационные ресурсы | | | |
| Врачебная тайна ИР | Да | Да | |
| ИР ПДн | Да | Да | |
| Служебные ИР | Да | Да | Да* |
| Технологические ИР | Да | Да | |
| Открытые информационные ресурсы медицинской организации | | | |
| Базовые государственные ИР | | Да | Да |

| | | | |
|---|---|---|---|
| Общедоступные ИР | | Да | Да |
| Инфраструктурные ИР | | Да | Да |

* Частично.

## 5.2. Основы построения системы обеспечения безопасности информации

### *5.2.1. Парадигма построения СОИБ*

Для формирования единой политики обеспечения ИБ, достижения требуемого уровня защищенности ИР медицинских организаций, оперативного реагирования на возникающие угрозы и негативные тенденции, создается система обеспечения безопасности информации, как комплекс мер и средств, направленных на выявление, противодействие и ликвидацию различных угроз безопасности информации.

Создание СОИБ направлено на достижение требуемого уровня доверия:

- к объектам информатизации МО, в том числе к телекоммуникационной инфраструктуре;
- к субъектам (обладатели информации, субъекты персональных данных, операторы ИС и персональных данных, правообладатели, пользователи, работники МО, персонал взаимодействующих организаций, вспомогательный персонал, разработчики и поставщики средств обработки информации и программного обеспечения);
- к правилам (эксплуатации и технической поддержки объектов информатизации МО, обслуживания, настройки и ремонта средств обработки информации, пользования и обмена информацией, учета и документирования событий);
- к аппаратной (средства обработки информации и вспомогательные технические средства и системы) и программной платформам объектов информатизации МО (ОС, специальное и прикладное ПО, средства защиты информации, СКЗИ);
- к телекоммуникационной инфраструктуре (каналообразующая аппаратура, концентраторы и коммутаторы, средства создания виртуальных частных сетей - VPN), в том числе выделенным и арендованным каналам связи.

В результате построения СОИБ, вокруг объектов защиты должна быть создана «оболочка», исключающая возможность модификации и любых несанкционированных действий с ними. При построении СОИБ требуется системное согласование средств и способов защиты и создание единой системы управления ИБ. Требуемый уровень безопасности объектов защиты МО достигается:

- локализацией ИР, требующих защиты;
- учетом всех субъектов информационных отношений и всех объектов защиты;
- доверенностью конфигурации и настроек ПО и технических средств ИС МО;
- целостностью всех элементов объектов информатизации МО и их окружения;
- подконтрольностью всех действий с объектами защиты;
- документированностью всех событий, влияющих на безопасность информации.

Локализация ИР, требующих защиты, достигается разделением ИС медицинских организаций на сегменты. При этом, рабочие станции пользователей, имеющих доступ к защищаемой информации одного уровня защищенности, средства отображения, хранения, обработки, ввода, вывода, коммутации и маршрутизации такой информации, равно как и сами ИР, содержащие такую информацию, должны быть обособлены в отдельный сегмент.

Сегменты могут группироваться по степени конфиденциальности, по функциональной потребности, по территориальному размещению средств обработки информации и самих ИР.

Сегментирование может проводиться как на физическом, так и на логическом уровне. Все сегменты сопрягаются между собой только через специальные средства защиты, установленные в точках их сопряжения. Количество точек сопряжения одного сегмента с другими должно быть минимально необходимым (ограниченным). Границей сегмента является внешний по отношению к сегменту порт коммутирующих (маршрутизирующих) устройств или средств защиты, установленных в точке сопряжения с другими сегментами.

Для обеспечения учета субъектов информационных отношений и объектов защиты, все субъекты (рабочие станции пользователей ИС МО, средства отображения, хранения, обработки, ввода, вывода, коммутации и маршрутизации, прикладные программы и приложения), независимо от степени конфиденциальности и критичности информации, к которым они имеют доступ (возможность обработки), и объекты защиты должны иметь уникальный идентификатор.

Создаваемая СОИБ должна обеспечивать персонификацию любых действий пользователей и администраторов ИС МО, контролируемый допуск к работе в ИС только зарегистрированных субъектов, прошедших процедуру аутентификации и блокировку работы любого субъекта, не имеющего регистрации.

Всем субъектам должны быть определены роли и полномочия по использованию ИР медицинской организации. Любые действия неавторизованными субъектами или субъектами, не имеющими соответствующих полномочий, должны блокироваться. Действия в ИС, не поддающиеся автоматической доверенной регистрации, должны осуществляться по правилу «двух рук», то есть должны выполняться только одновременно несколькими субъектами, предъявляющими соответствующие полномочия.

Доверенность конфигурации и настроек ПО и технических средств ИС обеспечивается тем, что все элементы ИС МО, задействованные в обработке защищаемой информации, оборудуются средствами, осуществляющими:

- контроль целостности и неизменности программного обеспечения при его загрузке и использовании;
- исключение возможности несанкционированной загрузки нештатной ОС, прикладных программ или утилит с внешних устройств ввода, в том числе использование командной строки и средств программирования, имеющихся в ИС;
- авторизацию и разграничение полномочий пользователей;
- блокирование несанкционированных процессов обработки защищаемых ИР и изменений правил доступа к ним.

Средства обеспечения доверенной загрузки должны обеспечивать контроль целостности общесистемного ПО, прикладных программ (приложений) и BIOS.

Целостность элементов объектов информатизации МО и их окружения достигается применением средств проверки подлинности и неизменности ПО, а также средств обнаружения и блокирования воздействия вредоносных программ и вирусов. Целостность средств обработки информации и помещений, в которых они размещаются, обеспечивается на физическом уровне.

Подконтрольность действий с объектами защиты и документированность событий, влияющих на безопасность информации, достигается постоянным мониторингом, сбором и

накоплением информации о событиях, которые могут повлиять на ИБ, в том числе мониторинг действий пользователей и администраторов ИС медицинских организаций, фактов загрузки и инициализации ОС, выдачи защищаемой информации на периферийное оборудование, попыток доступа процессов (сервисов) к защищаемым ИР или к объектам доступа (рабочие станции пользователей ИС МО, элементам телекоммуникационной инфраструктуры, периферийному оборудованию, томам, каталогам, файлам, записям, полям записей), попытки и факты изменений полномочий субъектов и статуса объектов защиты.

### *5.2.2. Состав и структура СОИБ*

СОИБ не является только технической системой, а объединяет три равнозначные составляющие, имеющие различные объекты воздействия:

- организационная база - система организационно-распорядительных документов, определяющих Политику ИБ, и персонал, выполняющий установленные правила защиты. Объектом воздействия этой составляющей СОИБ является персонал медицинских организаций и взаимодействующих организаций;
- исполнительный механизм - совокупность технических, программных и программно-аппаратных средств защиты информации, реализующих, независимо от места их установки, необходимые механизмы защиты. Объектом воздействия этой составляющей СОИБ являются технические, программные и программно-аппаратные средства, непосредственно реализующие механизмы (функции) защиты информации при ее обработке в ИС медицинских организаций;
- механизм поддержки - комплекс организационных и технических мер противодействия угрозам, осуществляемый различными структурными подразделениями МО, и обеспечивающий поддержку исполнения установленных правил и реализацию механизмов защиты. Объектом воздействия этой составляющей СОИБ являются организационные меры и вспомогательные средства объектов информатизации МО.

В целом, СОИБ создается как многоуровневая, иерархическая система, при этом, каждый уровень может иметь несколько слоев. Деление на уровни обусловлено тем, что в пределах каждого уровня выделяются разные группы задач обеспечения ИБ на объектах МО, решаемые относительно самостоятельно, но при условии использования результатов, достигнутых на остальных уровнях. В составе СОИБ выделяются 3 уровня: стратегический, оперативный, исполнительский.

Составляющие СОИБ размещаются на одном или нескольких уровнях. Такое размещение обусловлено тем, что элементы различных составляющих в совокупности могут решать одну группу задач обеспечения ИБ.

### *5.2.3. Организационная база СОИБ и рекомендации по ее формированию*

Организационную базу СОИБ составляют работники МО, которые реализуют и контролируют выполнение установленных правил обеспечения ИБ, применяя комплекс организационных и инженерно-технических мер противодействия угрозам в совокупности с техническими, программными и программно-аппаратными средствами защиты. В организационную базу СОИБ включаются:

- работники МО, должностные лица, штатные специалисты отделов информационной безопасности (работники, ответственные за ИБ), информационных технологий и связи МО (системные администраторы,

администраторы баз данных, администраторы безопасности информации), а также работники обеспечивающих подразделений (делопроизводства, кадров, жизнеобеспечения и энергоснабжения, физической и пожарной безопасности);

- персонал взаимодействующих организаций: сотрудники привлекаемых подразделений физической охраны объектов МО, специалисты операторов связи (провайдеров), сервисных организаций, поставщиков оборудования, а также организаций, разрабатывающих, отлаживающих и сопровождающих прикладное программное обеспечение для нужд ИС медицинских организаций;
- система организационно-распорядительных документов, определяющих Политику обеспечения ИБ, регламенты, положения, инструкции, определяющие роли и ответственность субъектов за обеспечение безопасности информации.

Общее руководство СОИБ и принятие всех решений по вопросам ее функционирования осуществляет БУ «Медицинский информационно-аналитический центр» Ханты-Мансийского автономного округа - Югры.

Подразделения информационной безопасности МО являются ключевыми элементом организационной базы, обеспечивающим подготовку предложений по совершенствованию и реализации положений Политики информационной безопасности, осуществляющим взаимодействие с подразделениями МО и контроль за выполнением установленных требований.

На этапе формирования организационной базы требуется уточнение функциональных обязанностей, прав и полномочий должностных лиц и работников МО в части обеспечения безопасности информации.

Для повышения эффективности защиты информации, целесообразно рассмотреть вопрос введения штатных должностей специалистов по информационной безопасности и администраторов информационной безопасности в МО.

Администраторы ИС медицинских организаций (системные администраторы, администраторы баз данных, администраторы безопасности информации) непосредственно реализуют мероприятия по защите ИР, применяют средства защиты, обеспечивают сопровождение объектов защиты, осуществляют контроль за ходом информационных процессов и разграничением доступа к объектам защиты (комплексное администрирование).

Работники МО, при координирующей роли подразделений ИБ, непосредственно реализуют комплекс организационных и технических мер противодействия угрозам, направленный на достижение требуемого уровня защищенности информации.

Пользователи ИС МО, независимо от их подчиненности, непосредственно руководствуются положениями Политики ИБ, принятой в МО, соблюдают установленные режимы защиты ИР, обеспечивают строгое исполнение предписанных правил безопасности информации.

Основой для разработки системы организационно-распорядительных документов являются результаты аудита безопасности информации, особенно, в части обследования управления безопасностью информации.

### *5.2.4. Исполнительный механизм СОИБ и рекомендации по его построению*

Создание исполнительного механизма СОИБ осуществляется методом технического проектирования системы защиты информации и системы активной защиты (при

необходимости) на основе анализа имеющихся угроз безопасности информации и выбора функций безопасности из числа стандартизированных, а также выполнения рекомендаций стандартов и руководящих документов, позволяющих устранить выявленные уязвимости. При проектировании исполнительного механизма СОИБ, должна быть явно показана устранимость той или иной угрозы (уязвимости) выбранными функциями безопасности.

Исполнительным механизмом СОИБ являются системы защиты информации ИС медицинских организаций и телекоммуникационной инфраструктуры, в состав которых включаются:

- встроенные в общесистемное программное обеспечение ИС медицинских организаций и телекоммуникационной инфраструктуры функции защиты информации (декларированные функции защиты ОС, СУБД, ПО средств телекоммуникационного и маршрутизирующего оборудования, прикладного ПО);
- специальные программные и программно-аппаратные средства защиты, используемые в ИС МО и телекоммуникационной инфраструктуры (средства защиты от НСД к информации, средства повышенной аутентификации, межсетевые экраны, СКЗИ, средства создания доверенных каналов связи, антивирусные средства и т.п.);
- средства контроля (мониторинга) состояния ИС МО, телекоммуникационной инфраструктуры и действий пользователей (сканеры сети, сканеры системы, средства контекстного анализа сообщений, средства контроля нежелательной активности пользователей, датчики технических средств охраны, противопожарной сигнализации и т.п.);
- средства управления ИБ в ИС медицинской организации и телекоммуникационной инфраструктуре (агенты управления, консоли администратора управления, средства регистрации и хранения данных контроля и т.п.).

СЗИ обеспечивают реализацию практических правил ИБ в ходе процесса обработки защищаемых ИР и может эффективно выполнять свои функции только при условии выполнения мер противодействия угрозам, реализуемых механизмом поддержки.

Создание исполнительного механизма СОИБ, в основном, сводится к техническому проектированию и построению СЗИ, соответствующей установленному уровню защищенности ИС МО, и осуществляется в ходе эскизного и технического проектирования (модернизации) ИС МО или отдельных их элементов (подсистем, приложений, сегментов).

В ходе проектирования (модернизации) проводится разработка предварительных проектных решений, технико-экономическое обоснование эффективности выбранных вариантов, разработка, монтаж, испытания, сертификация (при необходимости) и тестирование решений и используемых средств защиты информации. При необходимости проводится проектирование помещений с учетом требований нормативных документов по обеспечению ИБ.

### *5.2.5. Механизм поддержки СОИБ и рекомендации по его построению*

Создание механизма поддержки СОИБ осуществляется методом изучения и практического применения существующего передового опыта в области обеспечения безопасности информации, а также выбора необходимых мер защиты из числа рекомендованных:

- Федеральный закон от 27.07.2006 No 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 01.11.2012 №1119 «Требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Гостехкомиссия России «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»,
- ГОСТ Р ИСО/МЭК 15408-2002 «Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий»,
- ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;
- ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
- ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
- ГОСТ 34.602-89 «Информационная технология. Комплекс
- стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем»;
- Руководящий документ 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов»;
- международном стандарте ISO/IEC 27001 «Информационные технологии. Технологии безопасности. Система управления информационной безопасностью. Требования».
- Руководящий документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ России от 10 июля 2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные 8 Центром ФСБ России от 21 февраля 2008 года №149/54-144;
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 года №149/6/6-622.

Инженерно-технические меры, предусмотренные механизмом поддержки, рассматриваются в ходе проектирования строительства (реконструкции) зданий и помещений МО. При описании механизма поддержки, должна быть явно показана устранимость той или иной угрозы выбранными организационными и инженерно-техническими мероприятиями.

Механизм поддержки СОИБ составляет комплекс организационных, инженерно-технических и технических мер противодействия угрозам, осуществляемый различными подразделениями МО, действия которых координируются, управляются и контролируются. В состав механизма поддержки включают:

- комплекс организационных мероприятий: система экономического стимулирования, подбора и подготовки работников, система физической защиты объектов МО, разрешительная система допуска персонала, система учета материальных средств, система учета и реагирования на инциденты;
- комплекс инженерно-технических мер: система жизнеобеспечения объектов информатизации МО, системы противопожарной защиты и охранной сигнализации;
- комплекс технических мер: системы резервирования каналов связи телекоммуникационной инфраструктуры, критического оборудования ИС МО, система резервного гарантированного и бесперебойного энергоснабжения.

Состав организационных мероприятий определяется в организационно-распорядительной документации, а также исполнительной документацией по вопросам обеспечения ИБ (должностные положения и инструкции, эксплуатационные документы СЗИ, таблицы разграничения прав доступа к ИР).

К моменту создания СОИБ на объектах медицинских организаций, как правило, уже имеются развернутые и действующие системы пожарной и охранной сигнализаций, а также организована охрана помещений и прилегающих территорий. При создании СОИБ необходимо учитывать, что часть угроз могут быть минимизированы уже имеющимися на объектах МО техническими средствами и системами.

### *5.2.6. Система управления информационной безопасностью*

Для координации и контроля действий МО по реализации политики ИБ, в составе СОИБ, на основе соответствующих подразделений МО, формируется система управления ИБ, построение которой выполнено в соответствии с Концепцией построения системы управления информационной безопасностью МО.

Основу СУИБ составляет организационная база СОИБ, которая обеспечивает единую вертикаль управления всеми механизмами СОИБ из единого центра (принцип иерархичности управления) на всех жизненных циклах создания, передачи, обработки и хранения объектов защиты и эксплуатации ИС МО (принцип непрерывности управления).

Иерархичность СОИБ предполагает создание в МО, вертикальной структуры СУИБ, обеспечивающей проведение единого замысла обеспечения безопасности объектов защиты и автоматизированное документирование всех событий, влияющих на обеспечение ИБ с возможностью их последующего анализа (принцип доказательности). Для этого создается отдельная (структурно и физически) административная база данных СУИБ (принцип выделенности).

СУИБ, как правило, должна комплектоваться специалистами, имеющими практический опыт работы в области защиты информации и отвечающими соответствующим квалификационным требованиям для специалистов по комплексной защите информации. Их численность должна быть достаточна для обеспечения ИБ. Зачисление работников на временную работу не допускается.

### 5.3. Архитектура системы обеспечения информационной безопасности

#### *5.3.1. Архитектура организационной базы СОИБ*

Организационная база СОИБ строится как иерархически-матричная структура. Иерархичность предполагает создание в многоуровневой вертикальной структуры, позволяющей своевременно довести управляющее воздействие до исполнительных механизмов СОИБ и получить оперативную информацию о реакции на эти воздействия для последующего их анализа и коррекции.

Организационная база архитектурно имеет две составляющие: «Персонал» и «Политика». Первая составляющая определяется и напрямую зависит от организационно-штатной структуры, а вторая определяется пакетом организационно-распорядительных документов, направленных на формирование и реализацию Политики безопасности.

Подразделения ИБ медицинских организаций являются ядром организационной базы СОИБ и подчиняются непосредственно руководителю МО. Обязанности, права и полномочия работников подразделений ИБ определяются должностными регламентами. При администрировании безопасности информации в ИС МО должно обеспечиваться сопряжение функций администрирования безопасности информации с функциями системы администрирования процесса обработки информации (комплексное администрирование). Системные администраторы, администраторы баз данных ИС МО (подчиненные структурным подразделениям информатизации МО) непосредственно реализуют мероприятия по защите ИР, осуществляют контроль за ходом информационных процессов, обеспечением разграничения доступа к ИР в процессе их использования.

Администраторы безопасности информации взаимодействуют со всеми администраторами ИС, обеспечивающими формирование и сопровождение защищаемых ИР и контроль за информационными процессами.

Задачами администраторов безопасности информации являются:

- формирование и контроль списка пользователей ИС МО, допущенных к работе с каждым видом ИР;
- формирование параметров входа в ИС МО (идентификатора) и ключевых данных пользователей;
- контроль текущего состояния ИС МО, просмотр журнала активных сеансов, контроль за работой конкретных рабочих станций (АРМ) и конкретных пользователей ИС МО;

- контроль за действиями администраторов ИС МО (администраторов ИС, баз данных) по администрированию штатных (встроенных) для общесистемного ПО механизмов защиты;
- администрирование специализированных средств защиты информации и анализа защищенности ресурсов ИС МО, поддержка функционирования средств, технологий и процессов обеспечения ИБ МО;
- учет наступления системных событий, связанных с инициализацией функций ИС МО, изменением их конфигурации, а также изменением прав доступа пользователей и процессов.

Численность администраторов безопасности информации и специалистов по защите информации определяется масштабом ИС МО и объемом защищаемых ИР МО.

Для реализации задач обеспечения безопасности информации, в зависимости от организационно-штатной структуры МО, подразделения МО в составе СОИБ наделяются следующими полномочиями (но не ограничиваясь):

- управлять планами обеспечения ИБ МО;
- разрабатывать и вносить предложения по изменению Политики ИБ МО;
- изменять существующие и принимать новые организационно-распорядительные и нормативно-методические документы по обеспечению ИБ в МО;
- выбирать средства управления и обеспечения ИБ при эксплуатации ИС МО;
- контролировать действия пользователей ИС МО, в том числе пользователей, имеющих максимальные полномочия;
- контролировать активность пользователей ИС МО, связанную с доступом к ИР и использованием средств защиты информации;
- осуществлять мониторинг событий ИБ;
- расследовать нарушения ИБ и, в случае необходимости, выходить с предложениями по применению санкций в отношении лиц, осуществивших противоправные действия;
- участвовать в действиях по восстановлению работоспособности ИС МО после сбоев и аварий;
- создавать, поддерживать и совершенствовать СУИБ МО.

Конкретные полномочия подразделений МО, в том числе обеспечивающих подразделений (информатизации, делопроизводства, кадров, жизнеобеспечения и энергоснабжения, физической безопасности), по исполнению функций защиты информации определяются в организационно-распорядительном документе.

Совершенствование и развитие составляющей «Персонал» организационной базы СОИБ должно быть направлено на:

- увеличение штата работников подразделений ИБ Департамента здравоохранения и подведомственных медицинских организациях;
- создание в Департаменте здравоохранения и подведомственных медицинских организациях аппарата администраторов ИБ;
- оснащение подразделений ИБ программными и программно-техническими средствами мониторинга и контроля состояния ИБ в медицинских организациях;
- повышение квалификации и профессионализма работников МО, непосредственно задействованных в решении вопросов обеспечения ИБ.

Подготовка и переподготовка пользователей и специалистов по защите информации требует создания системы повышения уровня технической грамотности и информированности в области ИБ, а также переподготовки специалистов по защите информации. Для этого необходимо регулярно проводить тренинги для персонала и

контроль готовности новых работников по применению правил информационной защиты, а также периодически осуществлять переподготовку специалистов подразделений защиты информации. Особенно важно проводить тренинги при изменении конфигурации ИС МО (внедрении новых технологий и прикладных систем, смены оборудования, ключевых приложений, новых правил и инструкций).

Политика ИБ является собирательным понятием, предполагающим создание совокупности взаимоувязанных нормативных и организационно-распорядительных документов, как единых для всех участников информационного обмена (Общая политика), так и специализированных, для территориальных органов и подведомственных учреждений (Частная политика), и устанавливающих порядок обеспечения безопасности информации при осуществлении информационного обмена, управления и контроля ИБ, а также выдвигающих требования по поддержанию этого порядка.

Политика ИБ направлена на:

- нормативное урегулирование процесса обмена защищаемой информации между участниками информационного обмена;
- установление организационно-правового режима использования ИР МО, ответственность должностных лиц и работников за соблюдение этого режима;
- реализацию комплекса организационных, программных и аппаратно-программных мероприятий по обеспечению целостности, доступности и конфиденциальности защищаемой информации;
- предоставление участникам информационного обмена необходимых сведений для сознательного поддержания установленного уровня защищенности информации;
- организацию постоянного контроля эффективности принятых мер защиты и функционирования системы обеспечения ИБ;
- создание в ее территориальных органах резервов и возможностей по ликвидации последствий нарушения режима защиты информации и восстановления ИБ.

Дополнительно, документы, формирующие Частные политики в подведомственных медицинских организациях, должны определять:

- роли и ответственность работников МО за обеспечение ИБ;
- требования по соблюдению конфиденциальности;
- порядок классификации ИР;
- процедуры управления ИР МО в соответствии с установленными правилами разграничения доступа;
- порядок организации физической защиты объектов информатизации МО;
- порядок проведения регламентных работ и сервисного обслуживания на оборудовании ИС МО;
- порядок реагирования на инциденты и другие вопросы, необходимые для обеспечения требуемого уровня безопасности ИР.

На стратегическом уровне Политики ИБ формулируются цели обеспечения безопасности информации, которые в дальнейшем определяют правила и требования по всем вопросам безопасности информации и становятся обязательными для всех участников информационного взаимодействия.

Все последующие технические решения по развитию ИС и телекоммуникационной инфраструктуры и защите ИР, должны опираться на выводы данной Стратегии.

На исполнительном уровне Политики МО разрабатываются организационно-распорядительные документы, регламентирующие вопросы организации и проведения работ по защите информации, положений об инфраструктурных элементах системы обеспечения безопасности информации, разрешительной системе доступа исполнителей к документам и сведениям, регламентах выполнения защищенных информационных процессов, а также технические требования к составляющим элементам СЗИ. Такими документами являются:

- стандарты (Технические требования) по обеспечению ИБ в медицинских организациях;
- регламенты обеспечения ИБ в медицинских организациях.

Регламенты являются документами, отражающими организационную составляющую процесса обеспечения безопасности информации.

Регламент обеспечения ИБ устанавливает:

- правила обеспечения режима защиты конкретных ИР;
- правила регистрации пользователей и назначения им прав доступа;
- правила работы пользователей с защищаемыми ИР;
- порядок контроля режима защиты информации и реагирования на нарушения режима защиты (разбор инцидентов);
- порядок ликвидации последствий при возникновении нештатных ситуаций и нарушении установленного режима защиты.

Исполнительский уровень Политики ИБ объединяет исполнительную документацию, включающую должностные регламенты и инструкции, а также эксплуатационные документы средств защиты информации, обеспечивающих разграничение доступа к защищаемым ИР, средств мониторинга и контроля. Документы этого уровня основываются на эксплуатационной документации СЗИ и программных компонент.

### *5.3.2. Архитектура исполнительного механизма СОИБ*

Исполнительный механизм  отношений между субъектами и защищаемыми ИР.

Исполнительный механизм, непосредственно не влияя на информацию в процессе ее обработки, реализует свои функции через механизмы защиты элементов инфраструктуры и глубоко интегрирован в элементы ИС МО.

Исполнительный механизм СОИБ строится как матричная структура, позволяющая обеспечить надежные горизонтальные связи взаимодействия между отдельными СЗИ, встроенными функциями безопасности общесистемного и прикладного ПО, а также с элементами системы активной защиты (при необходимости). При этом должно обеспечиваться централизованное управление всеми процессами защиты информации.

Роль исполнительного механизма СОИБ исполняет СЗИ, которая строится как территориально распределенная централизованная автоматизированная система, которая может быть структурирована по следующим функциям:

- поддержки доверенной среды (ПДС);
- идентификации и аутентификации субъектов (ИАС);
- контроля и управления доступом субъектов (КДС);
- защиты потоков информации (ЗПИ);
- регистрации и аудита событий (РАС);
- управления информационной безопасностью (УИБ).

ПДС предназначен для поддержания целостной программно-аппаратной среды ИС МО и обеспечения гарантий доверительности пользователей при использовании предоставляемых сервисов и оказании государственных услуг. В состав ПДС также входят средства защиты от вредоносных программ и вирусов (антивирусные средства), которые охватывают два подуровня: пользовательский и сетевой.

ИАС предназначен для проведения процедур аутентификации/идентификации субъектов доступа, пользующихся ИС МО на всех этапах обработки и обращения в ней информации. ИАС должен обеспечивать поддержку процесса идентификации (аутентификации) пользователей ИС МО в случае использования субъектами доступа в качестве средств идентификации (аутентификации) цифровых сертификатов, а также в случае использования в ИС МО при межведомственном информационном обмене средств подтверждения (проверки) подлинности электронных документов (электронных подписей).

КДС предназначен для управления и контроля за доступом пользователей ИС МО к объектам защиты, АРМ, серверам, а также к прикладным системам и сервисам при исполнении им государственных функций и оказании государственных услуг.

ЗПИ предназначен для создания доверенных каналов связи между структурными элементами ИС МО, а также между ИС МО и другими взаимодействующими ИС.

РАС предназначен для оперативного оповещения специального подразделения и уполномоченных сотрудников (администраторы безопасности) МО, отвечающих за обеспечение ИБ о состоянии (изменениях) ПО и технических средств обработки информации, используемых в ИС МО, действиях администраторов и пользователей по конфигурированию ПО и технических средств обработки информации.

УИБ предназначен для оперативного управления отдельными контурами СОИБ и обеспечением безопасности информации в целом на основе установленных правил (политики) ИБ. Входящие в состав контуров элементы должны реализовывать функции безопасности, предусмотренные техническими требованиями Политики ИБ или аналогичными требованиями в объеме, необходимом для обеспечения требуемого уровня защищенности ИС МО.

Используемые в СЗИ средства защиты информации должны пройти оценку соответствия, подтверждающую выполнение ими специальных функций по защите, в соответствии с требуемым классом защищенности, а также (в зависимости от установленного класса защищенности) отсутствие не декларированных возможностей (для программных и программно-аппаратных средств).

Архитектура СЗИ не должна накладывать жестких ограничений на информационные технологии, используемые в ИС медицинских организаций и должна обеспечивать реализацию функций безопасности на всех этапах обработки информации, в том числе при техническом обслуживании и ремонте оборудования ИС медицинских организациях.

### *5.3.3. Архитектура механизма поддержки СОИБ*

Механизм поддержки СОИБ реализуется различными структурными подразделениями МО, которые, как правило, не участвуют непосредственно в процессе обработки информации или обслуживании ИС МО и не имеют единого подчинения на оперативном уровне. При этом всегда существуют широкие горизонтальные связи взаимодействия. Комплекс мер, реализуемых механизмом поддержки, направлен на

усиление мер, реализуемых исполнительным механизмом, поэтому механизм поддержки СОИБ строится по матричной структуре, аналогичной структуре исполнительного механизма СОИБ.

Меры, реализуемые механизмом поддержки СОИБ, структурируются по трем функциональным компонентам: организационная, инженерно-техническая и техническая.

Комплекс организационных мер составляют меры, определяемые организационно-распорядительными документами и направленные на поддержание установленного порядка обеспечения безопасности информации. Учитывая, что данные мероприятия напрямую не связаны с процессом обработки информации и, как правило, затрагивают наиболее общие для всех подразделений МО вопросы, состав определяющих их организационно-распорядительных документов не входит в Политику ИБ. Для формирования необходимых организационных мер требуется внесения изменений в действующие организационно-распорядительные документы.

Комплекс инженерно-технических мер составляют меры, направленные на поддержание необходимых условий работы ИС МО и обеспечение общей защиты объектов. Такие меры определяются нормативными документами, техническими условиями, конструкторской документацией на сооружения и системы жизнеобеспечения объекта информатизации медицинских организациях.

Комплекс технических мер составляют меры, направленные на создание и поддержание в постоянной готовности резервных мощностей, позволяющих обеспечить при необходимости быстрое устранение нештатных ситуаций при эксплуатации ИС МО.