УТВЕРЖДЕНО
приказом директора
ОГБУЗ «Областная больница»
от 10.12.2025 № 338-ОД

Политика информационной безопасности ОГБУЗ «Областная больница»

1. Общие положения

1.1. Настоящая Политика информационной безопасности (далее – Политика) является документом, определяющим направления деятельности в области обеспечения информационной безопасности, и представляет собой систематизированное изложение целей и задач информационной безопасности, как несколько правил, процедур, практических приемов и руководящих принципов, которыми руководствуется областное государственное бюджетное учреждение здравоохранения «Областная больница» (далее - медицинская организация), а также организационных, технологических и процедурных аспектов обеспечения информационной безопасности.

1.2. Политика разработана в соответствии с положениями:

- Федерального закона от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федерального закона от 26.07.2017г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Постановления Правительства РФ от 12.04.2018 г. № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями»;
- Постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа Федеральной службы по техническому и экспортному контролю от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказа Министерства здравоохранения РФ от 24.12.2018 г. № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций».

1.3. Основной целью обеспечения информационной безопасности медицинской организации являются действия, направлены на достижение защиты субъектов

информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию.

1.4. Основной задачей в области информационной безопасности медицинская организация признает совершенствование мер и средств обеспечения оптимального уровня информационной безопасности и защиты информации, обрабатываемой информационными системами медицинской организации в соответствии с требованиями действующего законодательства Российской Федерации, нормативных, методических и организационно-распорядительных документов уполномоченных органов Российской Федерации (регуляторов).

1.5. Обеспечение информационной безопасности, должно осуществляться в соответствии со следующими основными принципами:

- Принцип законности: при выборе мероприятий по защите информации, должно соблюдаться действующее законодательство Российской Федерации в сфере защиты информации. Все работники должны иметь представление об ответственности за правонарушения в сфере защиты информации. Программные и программно-аппаратные средства, применяемые в медицинской организации, должны иметь соответствующие лицензии, официально приобретаться у представителей разработчиков этих средств или являться интеллектуальной собственностью медицинской организации.

- Принцип системности: при создании системы защиты должны учитываться актуальные угрозы безопасности информации, возможные объекты и направления атак на неё со стороны нарушителей. Система защиты должна строиться с учетом не только известных каналов утечки информации, но и с учетом возможности появления новых уязвимостей в программном обеспечении.

- Принцип комплексности: комплексное использование средств защиты информации предполагает согласованное применение при построении целостной системы защиты, перекрывающей все существенные угрозы безопасности информации. Защита должна строиться эшелонировано. Физическая защита должна обеспечиваться физическими средствами и организационными мерами. При построении, внедрении и эксплуатации системы защиты информации руководство медицинской организации обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

- Принцип своевременности: разработка системы защиты информации должна вестись параллельно с разработкой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные информационные системы, обладающие достаточным уровнем защищенности.

- Принцип преемственности: постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и системы её защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите информации.

- Принцип достаточности: соответствие уровня затрат на обеспечение информационной безопасности и ценности информационных ресурсов на величину возможного ущерба от их разглашения, уничтожения и искажения. Используемые меры и

средства защиты информации не должны ухудшать эргономические показатели компонентов информационных систем.

- Принцип ответственности: возложение ответственности за обеспечение безопасности информации и её обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения был известен нарушитель.

- Принцип обоснованности и технической реализуемости: информационные технологии, программные и программно-аппаратные средства, меры защиты информации должны быть реализованы по современным решениям, обоснованы с точки зрения достижения заданного уровня защищенности информации и экономической целесообразности, а также соответствовать установленным нормам и требованиям по безопасности информации.

- Принцип профессионализма: реализация мер защиты информации и эксплуатация средств защиты информации должна осуществляться профессиональными специалистами. Привлечение специализированных организаций к разработке средств и реализации мер защиты информации, подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и лицензии на право оказания услуг в этой области.

- Принцип минимизации привилегий пользователей: обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих должностных обязанностей.

1.7. В целях обеспечения информационной безопасности медицинской организации при взаимодействии с контрагентами должно выполнять следующие мероприятия:

- заключение соглашения о неразглашении информации, содержащей сведения ограниченного распространения, полученной в ходе исполнения договорных обязательств;

- осуществление контроля за действиями представителей контрагентов в пределах контролируемой зоны медицинской организации.

1.8. Политика утверждается приказом директора медицинской организации и доводится до сведения всех работников медицинской организации.

1.9. Политика доступна всем пользователям информационных ресурсов медицинской организации.

2. Информационные системы медицинской организации и обеспечение информационной безопасности

2.1. К субъектам правоотношений, связанных с использованием информационных систем медицинской организации и обеспечением безопасности информации, относятся:

- медицинская организация, как обладатель информации;

- работники медицинской организации, как пользователи информационной системой медицинской организации в соответствии с возложенными на них должностными обязанностями;

- пациенты медицинской организации;

- работники организации, обеспечивающей эксплуатацию средств вычислительной техники, сетевой инфраструктуры и информационных систем медицинской организации;

- иные пользователи (физические и юридические лица), информация о которых накапливается, обрабатывается и хранится в информационных системах медицинской организации.

2.2. Объектами информационных отношений являются:

- информационные технологии и информационные ресурсы медицинской организации;

- медицинская информационная система «Пользовательский сегмент РМИС ЕАО» (МИС) и иные информационные системы, обеспечивающие функционирование организации (Приложение 1);

- процессы обработки информации в информационных системах;

- информационная инфраструктура, в том числе каналы связи и телекоммуникации;

- системы и средства защиты информации;

- объекты и помещения, в которых размещены средства обработки информации.

2.3. Медицинская информационная система и остальные информационные системы размещаются в разных сегментах локальной вычислительной сети медицинской организации, разделенных межсетевыми экранами.

2.4. Информационные системы, не относящиеся к медицинским, размещены в разных виртуальных сетях медицинской организации.

2.5. Конфиденциальная и открытая информация размещается на разных серверах медицинской организации.

2.6. Локальная вычислительная сеть защищается от внешнего проникновения и атак специализированным сетевым оборудованием.

2.7. Работники медицинской организации имеют доступ к информационным системам медицинской организации в соответствии с выполняемыми должностными обязанностями.

2.8. Работники организации, обеспечивающей эксплуатацию средств вычислительной техники, сетевой инфраструктуры и информационных систем медицинской организации, имеют доступ к вычислительной и оргтехнике, сетевому и серверному оборудованию медицинской организации.

2.9. Уровень доступа к информационной системе медицинской организации определяется для каждого работника индивидуально с соблюдением следующих требований:

- каждый работник имеет доступ только к той информации, которая необходима ему для выполнения должностных обязанностей;

- непосредственный руководитель работника имеет право на просмотр информации, используемой работником.

2.10 Категории лиц, участвующих в защите информации, их обязанности и функции:

- Руководитель медицинской организации:

- несет персональную ответственность за организацию защиты информации;
- утверждает Политику и другие организационно-распорядительные документы по защите информации в медицинской организации;
- выделяет необходимые ресурсы;
- назначает ответственных лиц.

- Лицо, ответственное за обеспечение информационной безопасности:

- организует реализацию требований Политики и всех документов по защите информации;
- координирует работу медицинской организации по защите информации;
- разрабатывает организационно-распорядительные документы;
- проводит внутренние проверки и расследует инциденты информационной безопасности;
- формируют запросы на предоставление/лишение прав доступа для сотрудников;
- организует обучение сотрудников медицинской организации в рамках информационной безопасности.

- Начальники отделов, заведующие отделениями:
  - определяют ценность информации в своих подразделениях;
  - обеспечивают соблюдение правил информационной безопасности подчиненными сотрудниками.
- Отдел информационной безопасности/Отдел информационных технологий/подрядные организации:
  - реализуют технические меры защиты (настройка СЗИ, антивирусы, межсетевые экраны, учетные записи);
  - осуществляют мониторинг и реагирование на инциденты информационной безопасности;
  - обеспечивают резервное копирование данных.
- Пользователи информационных систем (все сотрудники медицинской организации):
  - соблюдают все требования Политики информационной безопасности и всех нормативно-правовых документов по защите информации;
  - используют предоставленные средства защиты (пароли, электронные подписи);
  - немедленно сообщают о любых подозрительных ситуациях или инцидентах информационной безопасности ответственному за информационную безопасность или начальнику отдела информационной безопасности;
  - не разглашают конфиденциальную информацию.

2.11 Работники медицинской организации, как пользователи информационной системы медицинской организации, в соответствии с возложенными на них трудовыми обязанностями, обязаны соблюдать следующие требования:

- знать и соблюдать установленные требования по режиму обработки персональных данных, а также руководящих и организационно-распорядительных документов по работе со сведениями, содержащими персональные данные;
- соблюдать требования Инструкции по обеспечению защиты персональных данных, обрабатываемых в ИС «Пользовательский сегмент РМИС ЕАО» ОГБУЗ «Областная больница»;
- соблюдать требования Инструкции по организации парольной защиты в автоматизированных системах, предназначенных для обработки информации ограниченного распространения ОГБУЗ «Областная больница»;

- выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него инструкциями разработчика, размещенные в справочной системе «Единой цифровой платформы» (https://wiki.is-mis.ru).

- располагать во время работы экран монитора и принтера так, чтобы исключалась возможность несанкционированного ознакомления посторонними лицами с отображаемой на нём информацией;

- при отсутствии визуального контроля за компьютером доступ к нему должен быть заблокирован;

- не оставлять открытые помещения, в которых размещены средства вычислительной техники, без присмотра;

- в случае возникновения внештатных либо аварийных ситуаций принимать меры по реагированию с целью ликвидации их последствий в соответствии с инструкциями в рамках и в пределах возложенных на него функций.

2.12. Все работники под подпись ознакомлены с нормативными и организационно-распорядительными документами медицинской организации.

2.13. Все работники, допущенные к работе с информационной системой медицинской организации, ознакомлены под подпись с правилами и инструкцией по её использованию и несут персональную ответственность за их нарушение.

2.15. Работники медицинской организации несут персональную ответственность за нарушение правил и инструкций по передаче, обработке и хранению информации, содержащей сведения ограниченного распространения, в том числе врачебную тайну.

2.16. Обо всех выявленных нарушениях, связанных с информационной безопасностью и защитой информации, работники обязаны в кротчайший срок сообщить в отдел информационной безопасности медицинской организации.

2.17 Состав организационной системы управления деятельностью по защите информации и схема взаимодействия:

- Руководящий уровень: Директор медицинской организации/Комиссия по защите конфиденциальной информации.

- Организационно-управленческий уровень: Ответственный за обеспечение информационной безопасности.

- Исполнительный уровень:

- Руководители подразделений;
- Отдел информационной безопасности/Отдел информационных технологий;
- Отдел кадров.

- Пользовательский уровень: Все сотрудники медицинской организации.

Директор медицинской организации

↓ (утверждает политику, назначает, контролирует)

↓

Комиссия по защите конфиденциальной информации (рассматривает стратегию, инциденты, отчеты)

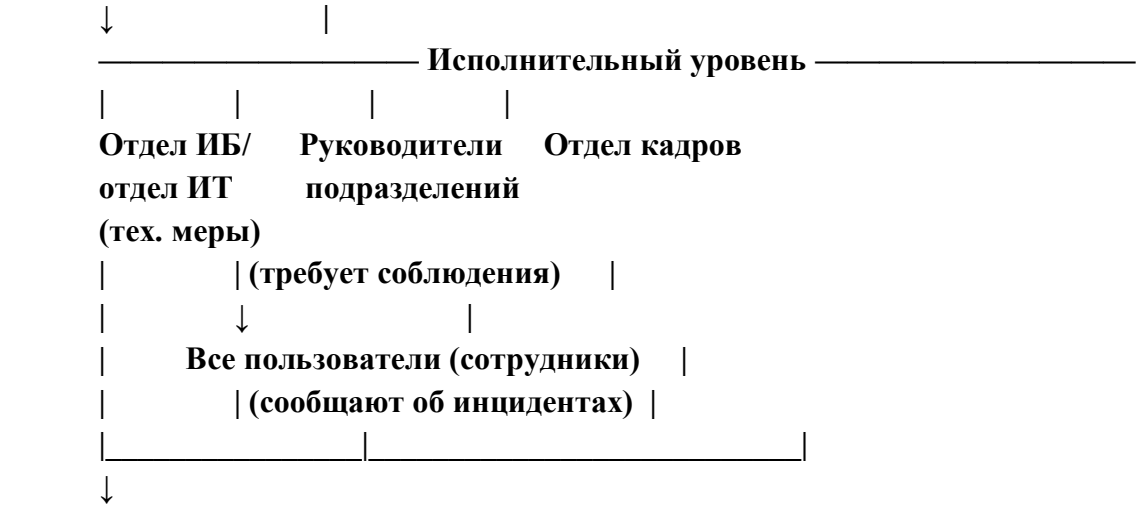
↑

↓

Ответственный за ИБ (координатор, разработчик, контролер)

| ↑

| (запросы, инциденты) | (требования, отчеты)



3. Требования, предъявляемые к медицинской информационной системе медицинской организации

3.1. «Пользовательский сегмент РМИС ЕАО» (далее – МИС) предназначена для сбора, хранения, обработки и представления информации, необходимой для автоматизации процессов оказания и учета медицинской помощи и информационной поддержки медицинских работников, включая информацию о пациентах, об оказываемой им медицинской помощи и о медицинской деятельности медицинской организации.

3.2. Посредством МИС обеспечивается:

- ведение электронной медицинской карты пациента;
- повышение эффективности лечения и повышение качества обслуживания клиентов;
- организация профилактики заболеваний, включая проведение диспансеризации, профилактических медицинских осмотров;
- мониторинг и управление потоками пациентов (электронная регистратура);
- оказание медицинской помощи с применением телемедицинских технологий;
- информационная поддержка принятия управленческих решений в медицинской организации;
- иные функциональные возможности.

3.3. Ведение электронной медицинской карты пациента в МИС включает:

- сбор, систематизацию и обработку сведений о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования при оказании медицинской помощи с ведением медицинской документации, указанных в статье 94 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- назначение диагностических исследований и формирование направления на диагностические исследования с рабочего места врача, реализованное для всех подразделений медицинской организации, получение результатов диагностических исследований в электронной форме, медицинских заключений и (или) ссылок на изображения из системы хранения результатов диагностических исследований (архив

медицинских изображений), которая может быть удаленной, самостоятельной и не входящей в состав МИС, полностью интегрированной с МИС МО или являться её частью;

- назначение лабораторных исследований и формирование направления на лабораторные исследования, получение результатов лабораторных исследований;

- учет временной нетрудоспособности (включая выдачу листка нетрудоспособности в форме электронного документа, логический контроль заполнения данных);

- реализацию индивидуальных программ реабилитации;

- выдачу медицинских заключений, справок.

3.4. Организация профилактики заболеваний включает:

- проведение диспансеризации, профилактических медицинских осмотров, иных профилактических мероприятий;

- учет граждан, прошедших профилактические медицинские осмотры, диспансеризацию;

- формирования списков граждан, которым необходимо пройти диспансеризацию, профилактические медицинские осмотры;

- выявление случаев, требующих реагирования и контроля предпринятых мер; _ мониторинг необходимости направления пациента на второй этап диспансеризации.

3.5. Мониторинг и управление потоками пациентов (электронная регистратура) включает:

- управление и планирование потоков пациентов при оказании первичной медико-санитарной помощи и специализированной медицинской помощи в амбулаторных и стационарных условиях (формирование расписания приема специалистов, учет и планирование занятости коечного фонда);

- мониторинг доступности записи на приём к врачу;

- мониторинг доступности медицинской помощи;

- учет оказанных медицинской организации услуг;

- направление информации об оказанных пациенту услугах в информационные системы территориального фонда обязательного медицинского страхования и страховых медицинских организаций.

3.6. Оказание медицинской помощи с применением телемедицинских технологий осуществляется в соответствии с Порядком организации и оказания медицинской помощи с применением телемедицинских технологий, утвержденным приказом Министерства здравоохранения РФ от 30 ноября 2017 г. № 965н, а также иных локальных актов с учетом установления экспериментального правового режима в сфере цифровых инноваций.

3.7. Информационная поддержка принятия управленческих решений в медицинской организации включает:

- автоматизированное формирование форм статистического учета и отчетности;

- работу системы поддержки деятельности руководителя медицинской организации, включая получение, формирование и представление форм статистического учета и отчетности, а также путем формирования аналитической справочной информации;

- автоматизацию учета запасов, списания лекарственных препаратов, специализированных продуктов лечебного питания и медицинских изделий и формирование отчетных форм для анализа информации о потребности в лекарственных препаратах, специализированных продуктах лечебного питания и медицинских изделиях.

4. Требования к организации защиты информации, содержащейся в информационных системах медицинской организации

4.1. В информационных системах медицинской организации объектами защиты являются:

- информация, содержащаяся в информационной системе;

- технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации);

- общесистемное, прикладное, специальное программное обеспечение, информационные технологии;

- средства защиты информации.

4.2. Для обеспечения защиты информации, содержащей персональные данные, медицинской организацией назначается должностное лицо (работник), ответственный за организацию обработки персональных данных. Организацией работ по защите информации в медицинской организации занимается отдел информационной безопасности.

4.3. Для проведения работ по защите информации в ходе создания и ввода в эксплуатацию информационной системы медицинской организацией в соответствии с законодательством Российской Федерации привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

4.4. Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4.5. Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) её создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы (далее - система защиты информации информационной системы).

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:

- неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

- неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

- неправомерного блокирования информации (обеспечение доступности информации).

4.6. Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в информационной системе;

- разработка системы защиты информации информационной системы;

- внедрение системы защиты информации информационной системы;

- обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

- обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

4.7. Формирование требований к защите информации, содержащейся в информационной системе, осуществляется медицинской организацией.

4.8. Формирование требований к защите информации, содержащейся в информационной системе, включает:

- принятие решения о необходимости защиты информации, содержащейся в информационной системе;

- классификацию информационной системы по требованиям защиты информации (далее -классификация информационной системы);

- определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;

- определение требований к системе защиты информации информационной системы.

4.9. При принятии решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется:

- анализ целей создания информационной системы и задач, решаемых этой информационной системой;

- определение информации, подлежащей обработке в информационной системе;

- анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;

- принятие решения о необходимости создания системы защиты информации информационной системе, а также определение целей и задач защиты информации в информационной системе, основных этапов создания системы защиты информации информационной системы и функций по обеспечению защиты информации, содержащейся в информационной системе медицинской организации и уполномоченных лиц.

4.10. Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации в соответствии с действующим законодательством РФ и нормативными документами регуляторов. Результаты классификации информационной системы оформляются актом классификации.

Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации.

4.11. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз

безопасности информации и последствий от нарушения свойств информации (доступности, целостности и конфиденциальности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в её отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности её функционирования.

Определение угроз безопасности информации проводится при подготовке технического задания на создание и/или изменение информационной системы, при изменении условий эксплуатации, а также периодически.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

5. Внедрение системы защиты информации информационной системы

5.1. Внедрение системы защиты информации информационной системы организуется отделом информационной безопасности медицинской организацией.

5.2. Внедрение системы защиты информации информационной системы осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

- установку и настройку средств защиты информации в информационной системе;
- внедрение организационных мер защиты информации;
- анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению;
- приемочные испытания системы защиты информации информационной системы.

5.3. Установка и настройка средств защиты информации в информационной системе должна проводиться в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и документацией на средства защиты информации.

5.4. При внедрении организационных мер защиты информации осуществляются:

- реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на доступ к информации и действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;
- отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

5.5. Анализ уязвимостей информационной системы проводится в целях оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.

Анализ уязвимостей информационной системы включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения информационной системы.

При анализе уязвимостей информационной системы проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением.

В случае выявления уязвимостей информационной системы, приводящих к возникновению дополнительных угроз безопасности информации, принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей.

6. Обеспечение защиты информации в ходе эксплуатации информационной системы

6.1. Обеспечение защиты информации в ходе эксплуатации информационной системы осуществляется медицинской организацией и включает следующие мероприятия:

- анализ угроз безопасности информации в информационной системе;
- планирование мероприятий по защите информации в информационной системе;
- управление (администрирование) системой защиты информации информационной системы;
- управление конфигурацией информационной системы и её системой защиты информации;
- информирование и обучение персонала информационной системы;
- реагирование на инциденты;
- контроль за обеспечением уровня защищенности информации, содержащейся в информационной системе.

6.2. В ходе анализа угроз безопасности информации в информационной системе осуществляются:

- выявление, анализ и устранение уязвимостей информационной системы;
- анализ изменения угроз безопасности информации в информационной системе;
- оценка возможных последствий реализации угроз безопасности информации в информационной системе.

Периодичность проведения указанных работ определяется медицинской организацией в организационно-распорядительных документах по защите информации, но не реже 1 раза в год.

6.3. В ходе планирования мероприятий по защите информации в информационной системе осуществляются:

- определение лиц, ответственных за реализацию и контроль мероприятий по защите информации в информационной системе;
- определение лиц, ответственных за выявление инцидентов и реагирование на них;
- разработка, утверждение и актуализация плана мероприятий по защите информации в информационной системе;
- определение порядка контроля выполнения мероприятий по обеспечению защиты информации в информационной системе, предусмотренных утвержденным планом.

6.4. В ходе управления конфигурацией информационной системы и её системы защиты информации осуществляются:

- определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и её системы защиты информации, и их полномочий, контроль за их действиями;

- определение компонентов информационной системы и её системы защиты информации, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю;

- управление изменениями информационной системы и её системы защиты информации;

- разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение защиты информации, санкционирование внесения изменений в информационную систему и её систему защиты информации, документирование действий по внесению изменений в информационную систему и сохранение данных об изменениях конфигурации;

- контроль действий по внесению изменений в информационную систему и её систему защиты информации.

6.5. Реализованные процессы управления изменениями информационной системы и её системы защиты информации должны включать процессы гарантийного и (или) технического обслуживания, в том числе дистанционного (удаленного), программных и программно-аппаратных средств, включая средства защиты информации, информационной системы.

6.6. В ходе реагирования на инциденты осуществляются:

- обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- своевременное информирование пользователями и администраторами лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе;

- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

- планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и её сегментов после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

6.7. В ходе информирования пользователей информационной системы осуществляются:

- информирование пользователей информационной системы о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации информационной системы;

- доведение до пользователей информационной системы требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений;

- контроль осведомленности пользователей информационной системы об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации.

Периодичность проведения практических занятий и тренировок с пользователями, мероприятий по обучению персонала и контролю осведомленности персонала устанавливается медицинской организацией в организационно-распорядительных документах по защите информации с учетом особенностей функционирования информационной системы, но не реже 1 раза в два года.

7. Обеспечение защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации

7.1. Обеспечение защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации осуществляется медицинской организацией в соответствии с эксплуатационной документацией на систему защиты информации информационной системы, нормативными и организационно-распорядительными документами по защите информации и в том числе включает:

- архивирование информации, содержащейся в информационной системе;

- гарантированное уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

7.2. Архивирование информации, содержащейся в информационной системе, осуществляется при необходимости дальнейшего использования информации в деятельности медицинской организации.

7.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для технического обслуживания, ремонта или утилизации.

7.4. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, содержащей сведения ограниченного распространения, и невозможности гарантированного уничтожения информации в соответствии с требованиями нормативных документов осуществляется физическое уничтожение этих машинных носителей информации.

8. Требования к защите информации, содержащейся в информационной системе

8.1. Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках её системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, её средств, систем связи и передачи данных.

8.2. При идентификации и аутентификации субъектов доступа и объектов доступа должно обеспечиваться присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

8.3. При управлении доступом субъектов доступа к объектам доступа должно обеспечиваться управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

8.4. При ограничении программной среды должна обеспечиваться установка и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

8.5. При защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должна быть исключена возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съёмных машинных носителей информации.

8.6. При регистрации событий безопасности должны обеспечиваться сбор, запись, хранение и защита информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

8.7. При антивирусной защите должно обеспечиваться обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

8.8. При обнаружении (предотвращении) вторжений должно обеспечиваться обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на

информационную систему и (или) информацию в целях её добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

8.9. При анализе защищённости информации должен обеспечиваться уровень защищённости информации, содержащейся в информационной системе, путем проведения мероприятий по защищённости информационной системы.

8.10. При обеспечении целостности информационной системы и информации должно обеспечиваться обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

8.11. При обеспечении доступности информации должен обеспечиваться авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

8.12. При защите среды виртуализации должен быть исключен несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

8.13. При защите технических средств должен быть исключен несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

8.14. При защите информационной системы, её средств, систем связи и передачи данных должны обеспечиваться защита информации при взаимодействии информационной системы или её отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по её системе защиты информации, направленных на обеспечение защиты информации.

8.15. Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

В информационных системах применяются средства защиты информации, сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК России, или на соответствие требованиям, указанным в технических условиях (заданиях по безопасности). При этом функции безопасности таких средств должны обеспечивать выполнение настоящих Требований.

9. Требования к программно-техническим средствам информационной системы медицинской организации

Программно-технические средства информационной системы медицинской организации должны:

- располагаться на территории Российской Федерации;

- в соответствии с действующим законодательством и нормативными документами быть сертифицированными Федеральной службой по техническому и экспортному контролю Российской Федерации и Федеральной службой безопасности Российской Федерации в отношении входящих в их состав средств защиты информации, включающих программно-аппаратные и программные средства защиты информации от несанкционированного доступа, антивирусное программное обеспечение, средства криптографической защиты информации и средства защиты информации от нелегитимного уничтожения, модификации и блокирования доступа к ней, а также от иных неправомерных действий в отношении обрабатываемых информационной системой данных;

- обеспечивать хранение медицинской документации в форме электронных документов, предусматривая резервное копирование медицинской документации в форме электронных документов и метаданных, восстановление медицинской документации в форме электронных документов и метаданных из резервных копий (ответственные ОГБУЗ «МИАЦ»);

- обеспечивать протоколирование и сохранение сведений о предоставлении доступа и о других операциях с документами и метаданными в автоматизированном режиме, а также автоматизированное ведение электронных журналов учета точного времени и фактов размещения, изменения и удаления информации, содержания вносимых изменений;

- функционировать в бесперебойном круглосуточном режиме, за исключением установленных периодов проведения работ по обслуживанию информационных систем и устранению неисправностей в работе, суммарная длительность которых не должна превышать 4 часов в месяц (за исключением перерывов, связанных с обстоятельствами непреодолимой силы) (ответственные ОГБУЗ «МИАЦ»);

- обеспечивать информационное взаимодействие информационных систем между собой путём обмена информационными сообщениями посредством формирования, отправки, получения, обработки запросов и ответов, форматы которых разрабатываются операторами информационных систем в сфере здравоохранения на основе справочников и классификаторов, содержащихся в федеральном реестре нормативно-справочной информации в сфере здравоохранения;

- обеспечивать достоверность и актуальность сведений о медицинской организации и медицинских работниках посредством информационного взаимодействия с федеральным реестром медицинских организаций, федеральным регистром медицинских работников Единой системы (ответственные отдел кадров);

- обеспечивать возможность ведения медицинской документации в форме электронных документов.

10. Обеспечение информационной безопасности персональных данных

10.1. Защита, хранение, обработка и передача персональных данных работников и пациентов медицинской организации осуществляется с соблюдением требований регламентируется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

10.2. Персональные данные работника - информация, необходимая медицинской организации в связи с трудовыми отношениями и касающаяся конкретного работника.

Персональные данные пациента - информация, полученная медицинской организацией при заключении с пациентом/заказчиком договора на оказание медицинских услуг, а также информация, полученная в процессе оказания медицинской помощи.

10.3. Состав обрабатываемых персональных данных Субъектов определены в Политике обработки и защиты персональных данных в ОГБУЗ Областная больница» и Политике обработки персональных данных в информационной системе «Пользовательский сегмент РМИС ЕАО» ОГБУЗ «Областная больница».

10.4. Все персональные сведения о работниках и пациентах медицинская организация может получить только от них самих. В случаях, когда медицинская организация получает необходимые персональные данные работников и пациентов только у третьего лица, медицинская организация уведомляет об этом работников и пациентов и получает от них письменное согласие.

10.5. Медицинская организация сообщает работникам и пациентам о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа работников и пациентов дать письменное согласие на их получение.

10.6. Персональные данные работников и пациентов являются конфиденциальной информацией и не могут быть использованы медицинской организацией или любым иным лицом в личных целях.

10.7. При определении объёма и содержания персональных данных работников и пациентов медицинская организация руководствуется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, иными федеральными законами.

10.8. Работники и пациенты не должны отказываться от своих прав на сохранение и защиту тайны.

10.9. Работодатель обрабатывает в информационных системах с использованием средств автоматизации определенные категории персональных данных работника, обеспечивает их защиту с учетом определенного типа угроз безопасности и уровня защищенности персональных данных.

10.10. Медицинская организация обрабатывает в информационных системах с использованием средств автоматизации, определенные персональных данных пациента, обеспечивает их защиту с учетом определенного типа угроз безопасности и уровня защищенности персональных данных.

10.11. Медицинская организация принимает организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах, предусмотренные Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

При защите персональных данных медицинская организация:

- обеспечивает режим безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечивает сохранность носителей персональных данных;

- утверждает перечень работников, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

10.12. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных медицинская организация осуществляет блокирование неправомерно обрабатываемых персональных данных с момента такого обращения на период проверки.

10.13. В случае выявления неточных персональных данных при обращении субъекта персональных данных медицинская организация осуществляет блокирование персональных данных с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных медицинская организация на основании сведений, представленных субъектом персональных данных, или иных необходимых документов, уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

10.14. В случае если обеспечить правомерность обработки персональных данных невозможно, медицинская организация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

10.15. В случае достижения цели обработки персональных данных медицинская организация прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

10.16. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных медицинская организация прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

10.17. Об уничтожении персональных данных медицинская организация уведомляет субъекта персональных данных.

10.18. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном Федеральными законами.

10.19. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

11. Обеспечение безопасности информации, содержащей врачебную тайну

11.1. Информация, содержащей врачебную тайну, — это информация о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иных сведений, полученных при его медицинском обследовании и лечении.

11.2. Не допускается разглашение информации, составляющей врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при исполнении трудовых, должностных, служебных и иных обязанностей, за исключением случаев, установленных Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

11.3. Врач, лица, участвующие в оказании медицинской помощи или пользующиеся правом доступа к медицинской информации, обязаны сохранять врачебную тайну, как и сам факт обращения за медицинской помощью, если пациент либо его законный представитель не распорядился иначе.

Врач должен следить за тем, чтобы лица, принимающие участие в лечении пациента, также соблюдали профессиональную тайну.

11.4. Врачебная тайна соблюдается в процессе научных исследований, обучения студентов и усовершенствования врачей. Демонстрация пациента возможна только с его согласия.

11.5. В целях сохранения врачебной тайны медицинская организация:

- устанавливает различные уровни доступа должностных лиц к информации, содержащей врачебную тайну;
- обеспечивает безопасность информационной системы в соответствии с положениями настоящей Политики информационной безопасности.

Охрана врачебной тайны является обязанностью всех работников медицинской организации, имеющих к ней прямое отношение.

11.6. Передача сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях допускается с письменного согласия гражданина или его законного представителя. Согласие на разглашение сведений, составляющих

врачебную тайну, может быть выражено также в информированном добровольном согласии на медицинское вмешательство.

11.7. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается исключительно в установленных действующим законодательством РФ случаях.

11.8. Неправомерное разглашение врачебной тайны влечет за собой дисциплинарную, административную, гражданскую и уголовную ответственность.

Мера ответственности работника за разглашение врачебной тайны определяется индивидуально, с учетом всех имеющих значение обстоятельств, включая:

- сами обстоятельства разглашения;
- цели разглашения;
- наличие возможности обойтись без такого разглашения;
- отношение пациента к факту разглашения (требует ли он защиты своих прав, нарушенных таким разглашением);
- последствия, которые в связи с таким разглашением наступили для гражданина и для медицинской организации (например, была ли на неё возложена обязанность возместить пациенту вред, причиненный разглашением врачебной тайны её работником).

11.9. Факт разглашения врачебной тайны фиксируется в акте, который составляется в произвольной форме в присутствии не менее чем двух свидетелей, либо в докладной записке, которую составляет лицо, выявившее факт разглашения врачебной тайны.

11.10. На основании акта или служебной записки создается комиссия и проводится внутреннее расследование с целью установления виновности работника в разглашении сведений, составляющих врачебную тайну.

11.11. По результатам расследования медицинская организация принимает решение о возможности применения меры дисциплинарной ответственности. В случае положительного решения медицинская организация запрашивает у работника, допустившего разглашение врачебной тайны объяснение причин его поступка. На представление объяснений работнику дается 2 (два) рабочих дня. Запрос оформляется письменно.

Если по истечении 2 (двух) рабочих дней работник не предоставляет объяснения или отказывается объяснять причины разглашения врачебной тайны, медицинская организация составляет акт об отказе дать объяснения.

11.12. Оценив причины, указанные в объяснительной (акте об отказе дать объяснения), медицинская организация принимает решение об увольнении работника или вынесении выговора.

В случае увольнения издается приказ. С приказом об увольнении работника нужно ознакомить под подпись. Если довести до его сведения приказ невозможно, то на приказе делается соответствующая запись.

Приложение 1
к политике информационной безопасности

Перечень информационных систем,
эксплуатируемых в ОГБУЗ «Областная больница»

№	Наименование информационной системы	Тип (ИС, ГИС)	Назначение
1	1С: Зарплата и Кадры	ИС	введение кадрового и бухгалтерского учета
2	"Пользовательский сегмент РМИС ЕАО"	ИС	предназначена для ведения медицинской документации в электронном виде
3	1 С: Медицина. Больничная аптека	ИС	предназначена для автоматизации учета движения аптечных товаров внутри медицинской организации
4	Poliklinika_Учет медицинских услуг	ИС	предназначена для формирования отчетности
5	КЛЕРК 96. Расчет заработной платы	ИС	предназначена для расчета заработной платы сотрудников