Министерство здравоохранения
Удмуртской республики
бюджетное учреждение здравоохранения
Удмуртской Республики
«Республиканская офтальмологическая клиническая больница Министерства здравоохранения Удмуртской Республики»

П Р И К А З

13.07.2026 № 88/01-04

г. Ижевск

Об утверждении политики защиты информации

В соответствии с требованиями Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказа Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных учреждений», в целях определения единых принципов, подходов, целей при разработке, планировании, реализации, оценке и совершенствовании мероприятий и мер по защите информации в бюджетном учреждении здравоохранения Удмуртской Республики «Республиканская офтальмологическая клиническая больница Министерства здравоохранения Удмуртской Республики» (далее – Учреждение), п р и к а з ы в а ю:

1. Утвердить политику защиты информации в Учреждении (далее — Политика) согласно приложению к настоящему приказу.

2. Установить, что положения Политики обязательны для исполнения всеми работниками Учреждения в части, их касающейся.

3. Начальнику отдела кадров Федоровой И.М.:

– включить Политику в перечень локальных нормативных актов, обязательных для ознакомления работниками при приёме на работу до подписания трудового договора.

– организовать ознакомление принимаемых работников с указанной Политикой под роспись в листе ознакомления с локальными нормативными актами при приёме на работу до подписания трудового договора.

4. Руководителям структурных подразделений Учреждения ознакомить работников с положениями Политики в части, их касающейся, под роспись в листах ознакомления.

5. Начальнику отдела технического обеспечения Попову Р. Л. на постоянной основе организовать ознакомление организаций, которым предоставляется доступ к информационной системе Учреждения и (или) содержащейся в ней информации для оказания услуг, проведения работ по обработке, хранению информации, созданию (развитию), обеспечению эксплуатации информационной системы, с положениями Политики в части, их касающейся.

6. Секретарю отдела кадров Шинкарецкой Е.А. довести настоящий приказ до заместителей главного врача, руководителей структурных подразделений Учреждения установленным порядком.

7. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач А.В. Сорокин

Приказ вносит:
Специалист по защите информации
_____О.П. Химчак

Согласовано:
Начальник отдела технического обеспечения
_____Р.Л. Попов

Заместитель главного врача по организационно-методической работе
_____Е.В. Леонова

Приложение

УТВЕРЖДЕНО
приказом БУЗ УР «РОКБ МЗ УР»
от 13.07.2026 № 88/01-04

Политика защиты информации в бюджетном учреждении здравоохранения Удмуртской Республики «Республиканская офтальмологическая клиническая больница Министерства здравоохранения Удмуртской республики»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика защиты информации (далее – Политика) является основополагающим документом деятельности по защите информации в бюджетном учреждении здравоохранения Удмуртской Республики «Республиканская офтальмологическая клиническая больница Министерства здравоохранения Удмуртской республики» (далее – Учреждение). Политика определяет единые принципы, подходы, цели и организационную структуру при разработке, планировании, реализации, оценке и совершенствовании мероприятий и мер по защите информации.

1.2. Политика разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказом Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных учреждений» (далее – приказ ФСТЭК России от 11 апреля 2025 г. № 117) и иными нормативными правовыми актами Российской Федерации в области защиты информации.

1.3. В настоящей Политике используются следующие основные термины и определения:

– **защита информации** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

– **информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств;

– **ответственный за организацию защиты информации** – заместитель руководителя Учреждения, ответственное за организацию деятельности по защите информации, управление деятельностью по защите информации, а также организацию контроля за данной деятельностью;

– **подрядная организация** – организация, которой предоставляется доступ к информационным системам Учреждения и (или) содержащейся в них информации для оказания услуг, проведения работ по обработке, хранению информации, созданию (развитию), обеспечению эксплуатации информационных систем, а оказания услуг по защите информации;

– **показатель защищённости Кзи (показатель Кзи)** – показатель, характеризующий текущее состояние защиты информации от базового уровня угроз безопасности информации;

– **показатель уровня зрелости Пзи (показатель Пзи)** – показатель, который определяет достаточность и эффективность проведения мероприятий по защите информации;

– **специализированная организация** – организация, имеющая лицензию на деятельность по технической защите конфиденциальной информации и привлекаемая Учреждением для проведения мероприятий и принятия мер по защите информации;

– **специалист по защите информации** – работник Учреждение, выполняющее непосредственные функции по защите информации (реализующее меры и (или) мероприятия по защите информации);

– **угроза безопасности информации** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

– **ФСБ России** – Федеральная служба безопасности Российской Федерации;

– **ФСТЭК России** – Федеральная служба по техническому и экспортному контролю Российской Федерации.

1.4. Политика вступает в силу с момента её утверждения главным врачом и действует до утверждения новой редакции.

1.5. Политика обязательна для исполнения всеми сотрудниками Учреждения в части, их касающейся. Все сотрудники Учреждения должны быть ознакомлены с положениями настоящей Политики под роспись в листах ознакомления.

1.6. Подрядные (в том числе специализированные) организации должны быть ознакомлены с Политикой в части, их касающейся. Обязанность указанных организаций по выполнению Политики должна быть определена в документах Учреждения, на основании которых в том числе передаётся информация, предоставляется доступ к информационной системе Учреждения или содержащейся в ней информации.

1.7. Политика подлежит пересмотру и, при необходимости, изменению в следующих случаях:

– при изменении законодательства Российской Федерации в области защиты информации;

– при планировании изменений организационной структуры, сфер (видов) деятельности Учреждения и (или) изменений в информационных системах и информационно-телекоммуникационной инфраструктуре.

1.8. В целях обеспечения целостности и согласованности требований внесение изменений (корректировок) в настоящую Политику осуществляется путём утверждения её новой редакции.

2. ОБЛАСТЬ ДЕЙСТВИЯ ПОЛИТИКИ

2.1. Политика применяется для защиты информации в Учреждении в соответствии с приказом ФСТЭК России от 11 апреля 2025 г. № 117 и устанавливает требования к:

2.1.1. Информационным системам Учреждения (за исключением информационных систем, осуществляющих обработку информации, содержащей сведения, составляющие государственную тайну), включённым в перечень, утверждённый в соответствии с пунктом 5.3 настоящей Политики;

2.1.2. Защите информации следующих видов:

– информация, подлежащая защите, доступ к которой не ограничен законодательством;

– общедоступная информация;

– персональные данные.

2.1.3. Информационно-телекоммуникационной инфраструктуре, обеспечивающей функционирование информационных систем, попадающих в область действия настоящей Политики в соответствии с пунктом 2.1.1.

2.2. Политика применяется на всех стадиях (этапах) обработки и хранения информации, создания и развития (модернизации), эксплуатации и вывода из эксплуатации информационных систем.

2.3. Обработка в информационных системах информации, содержащей персональные данные, и её защита осуществляется в соответствии с законодательством Российской Федерации о персональных данных, а также с учётом положений настоящей Политики в части, не противоречащей ему.

2.4. Защита информации в информационных системах, являющихся значимыми объектами критической информационной инфраструктуры, осуществляется в соответствии с законодательством Российской Федерации о безопасности критической информационной инфраструктуры Российской Федерации, а также с учётом положений настоящей Политики в части, не противоречащей ему.

2.5. При использовании шифровальных (криптографических) средств защиты информации применяются требования, установленные ФСБ России, а также положения настоящей Политики.

3. ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Учреждение обеспечивает защиту информации в целях:

– недопущения (снижения возможности) наступления негативных последствий (событий) от нарушения конфиденциальности, целостности, доступности информации;

– недопущения (снижения возможности) наступления негативных последствий (событий) от нарушения функционирования информационных систем вследствие реализации (возникновения) угроз безопасности информации.

3.2. Для достижения поставленных целей в Учреждении решаются следующие задачи:

3.2.1. Организация деятельности, управление рисками и совершенствование защиты информации.

Включает:

– определение лиц, ответственных за защиту информации;

– инвентаризацию, идентификацию объектов защиты и классификацию информационных систем в соответствии с Приложением к Требованиям о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений (далее – Требования), утверждённым приказом ФСТЭК России от 11 апреля 2025 г. № 117;

– выявление и оценку угроз безопасности информации, реализация (возникновение) которых может привести к нарушению целей защиты информации;

– разработку, утверждение, внедрение и актуализацию документации по защите информации (настоящей Политики, стандартов, регламентов и иных локальных актов);

– планирование, контроль, регулярную оценку состояния защиты (показатели Кзи и Пзи) и совершенствование деятельности по защите информации;

3.2.2. Реализация технических мер защиты информации. Включает внедрение и сопровождение программных и программно-аппаратных средств для защиты информации, обеспечивающих, как минимум:

– защиту от несанкционированного доступа;

– антивирусную защиту;

– фильтрацию сетевого трафика и безопасное межсетевое взаимодействие;

– защиту информации от компьютерных атак, направленных на отказ в обслуживании;

– защиту виртуальной инфраструктуры;

– криптографическую защиту информации (при необходимости);

3.2.3. Управление доступом к информационным системам и информации. Включает:

– управление идентификацией, аутентификацией и авторизацией пользователей с соблюдением принципа минимальных привилегий;

– обеспечение безопасного удалённого и беспроводного доступа;

– особый контроль за предоставлением и использованием привилегированного доступа;

– управление жизненным циклом учётных записей, выданных сотрудникам Учреждения, подрядным (в том числе специализированным) организациям;

3.2.4. Обеспечение доступности, целостности и физической защиты. Включает:

– контроль конфигураций и управление обновлениями программного обеспечения;

– организацию резервного копирования и восстановления информации;

– мероприятия по обеспечению непрерывности функционирования информационных систем;

– физическую защиту средств обработки и хранения информации, линий связи;

3.2.5. Операционное реагирование и формирование культуры безопасности. Включает:

– мониторинг информационной безопасности, сбор и анализ событий безопасности;

– выявление, регистрацию, расследование и ликвидацию последствий инцидентов;

– повышение осведомлённости и обучение пользователей по вопросам защиты информации, в том числе с помощью имитационных рассылок и тренировок;

3.2.6. Обеспечение соответствия и подтверждение достаточности принятых мер.

Включает:

– выбор и реализацию мер защиты информации в соответствии с пунктами 62, 69 и 70 Требований, утверждённых приказом ФСТЭК России от 11 апреля 2025 г. № 117;

– аттестацию государственных информационных систем на соответствие требованиям приказа ФСТЭК России от 11 апреля 2025 г. № 117 в соответствии с Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утверждённым приказом ФСТЭК России от 29 апреля 2021 г. № 77. Аттестация иных информационных систем, попадающих в область действия настоящей Политики, осуществляется по решению ответственного за организацию защиты информации;

– применение сертифицированных средств защиты информации, обеспеченных технической поддержкой от производителя, в соответствии с пунктом 72 Требований, утверждённых приказом ФСТЭК России от 11 апреля 2025 г. № 117;

3.2.7. Взаимодействие с государственными системами.

Включает организацию и поддержание:

– непрерывного взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак в целях оперативного получения информации об угрозах и инцидентах;

– взаимодействия в автоматизированном режиме с Центром мониторинга и управления сетью связи общего пользования для обеспечения защиты от компьютерных атак, направленных на отказ в обслуживании.

3.3. Мероприятия и меры по защите информации в Учреждении направлены на недопущение следующих негативных последствий (событий), определённых на основе анализа деятельности Учреждения и банка данных угроз ФСТЭК России:

3.3.1. Ущерб физическом лицу:

– разглашение персональных данных граждан;

– нарушение неприкосновенности частной жизни;

– нарушение личной, семейной тайны, утрата чести и доброго имени;

– нарушение иных прав и свобод гражданина, закреплённых в Конституции Российской Федерации и федеральных законах;

– финансовый, иной материальный ущерб физическому лицу;

– нарушение конфиденциальности (утечка) персональных данных.

3.3.2. Ущерб деятельности Учреждению:

– невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций);

– необходимость изменения (перестроения) внутренних процедур целей, решения задач (реализации функций);

– принятие неправильных решений;

– утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.);

– нарушение законодательства Российской Федерации;

– необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций;

– недополучение ожидаемой (прогнозируемой) прибыли;

– необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств);

– нарушение деловой репутации;

– причинение имущественного ущерба;

– публикация недостоверной информации на веб-ресурсах организации;

– использование веб-ресурсов для распространения и управления вредоносным программным обеспечением.

3.3.3. Ущерб государству:

– возникновение ущерба бюджетам Российской Федерации;

– утечка информации ограниченного доступа;

– публикация недостоверной социально значимой информации на веб-ресурсах, к оторая может привести к социальной напряжённости, панике среди населения и др.

4. ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Деятельность по защите информации в Учреждении основывается на следующих ключевых принципах:

4.1.1. Законность: все мероприятия и меры по защите информации осуществляются в соответствии с законодательством Российской Федерации, нормативными правовыми актами федеральных органов исполнительной власти и национальными стандартами;

4.1.2. Поддержка основной деятельности: мероприятия и меры по защите информации разрабатываются и реализуются для обеспечения и содействия достижению целей основной деятельности. Защита информации направлена на создание и поддержание доверенной среды, необходимой для эффективного и непрерывного выполнения служебных задач;

4.1.3. Разумная достаточность: проводимые мероприятия и принимаемые меры по защите информации адекватны и соразмерны рискам (негативным последствиям) и актуальным угрозам безопасности информации, а также возможному ущербу от их реализации;

4.1.4. Превентивность: мероприятия проводятся и меры принимаются заблаговременно: приоритет отдаётся недопущению реализации актуальных угроз (посредством управления уязвимостями, контроля доступа, повышения осведомлённости), а не только ликвидации их последствий;

4.1.5. Непрерывность: защита информации обеспечивается на всех стадиях жизненного цикла информационных систем (создание, развитие (модернизация), ввод в эксплуатацию, эксплуатация, вывод из эксплуатации) и на всех этапах обработки информации;

4.1.6. Комплексность: проводимые мероприятия и принимаемые меры по защите информации включают правовые, организационные, программные, программно-аппаратные и физические средства, обеспечивающие взаимосвязанную защиту информации от актуальных угроз безопасности информации;

4.1.7. Централизация: управление деятельностью осуществляется централизованно через ответственного за организацию защиты информации и специалиста по защите информации, обладающих необходимыми полномочиями и ресурсами для планирования, контроля и координации соответствующих мероприятий в Учреждении;

4.1.8. Минимальные привилегии: доступ сотрудникам Учреждения, представителям подрядных (в том числе специализированных) организаций к информационным ресурсам предоставляется строго в объёме, необходимом для выполнения ими закреплённых за ними должностны х обязанностей (функций), договорных обязательств;

4.1.9. Постоянное совершенствование: деятельность по защите информации подлежит регулярной оценке на основе показателей Кзи и Пзи, пересмотру и улучшению на основе мониторинга ее эффективности, изменений в угрозах, технологиях и законодательстве Российской Федерации;

4.1.10. Персональная ответственность: все сотрудники Учреждения несут персональную ответственность за соблюдение положений настоящей Политики и иных локальных актов Учреждения по защите информации.

5. ОБЪЕКТЫ ЗАЩИТЫ

5.1. Объектами защиты в Учреждении являются информационные активы и компоненты информационно-телекоммуникационной инфраструктуры, несанкционированный доступ к которым и (или) воздействие на которые могут привести к нарушению целей защиты информации, установленных настоящей Политикой.

5.2. К объектам защиты относятся:

5.2.1. *Информация* – информация, доступ к которой ограничен законодательством либо внутренними документами Учреждения, и служебная информация (сведения о конфигурации информационных систем и сетей, сведения о событиях безопасности и др.);

5.2.2. *Информационная система* – информационная система, определённая в соответствии с п. 5.3 настоящей Политики;

5.2.3. *Информационно-телекоммуникационная инфраструктура* – программные и программно-аппаратные средства обработки и хранения информации, включая, но не ограничиваясь:

– серверы и серверное оборудование;

– автоматизированные рабочие места пользователей, использующих информационные системы, пользователей, обеспечивающих эксплуатацию информационных систем, специалиста по защите информации;

– периферийные устройства (многофункциональные устройства, принтеры, сканеры, видеокамеры, микрофоны и др.);

– микропрограммное, системное и прикладное программное обеспечение;

– оборудование (маршрутизаторы, коммутаторы, медиаконвертеры, трансиверы, мосты, шлюзы, ретрансляторы, сетевые адаптеры и др.) и физические линии связи, образующие корпоративную среду передачи данных;

– съёмные машинные носители информации (флэш-накопители, внешние накопители на жёстких дисках и др.);

– обеспечивающие системы;

5.2.4. *Средства защиты информации, в том числе криптографические.*

5.3. Конкретный перечень объектов защиты с указанием их классификационных признаков (класс защищённости, вид информации, категория объекта защиты) утверждается локальным актом Учреждения и подлежит периодической актуализации.

5.4. Утверждённый перечень объектов защиты является первичным документом для управления деятельностью по защите информации и служит основой для всех процессов защиты информации: оценки угроз безопасности информации, управления рисками, планирования мероприятий и реализации мер защиты информации.

5.5. Информационные системы Учреждения, включённые в перечень, утверждённый в соответствии с пунктом 5.3 настоящей Политики, подлежат классификации в соответствии с приложением к Требованиям, утверждённым приказом ФСТЭК России от 11 апреля 2025 г. № 117, для определения базовых мер защиты информации.

5.6. Результаты классификации оформляются актом классификации информационной системы Учреждения, который утверждается главным врачом. Акт классификации должен содержать наименование классифицируемой системы и сегментов информационной системы при их наличии, уровень значимости информации, обрабатываемой в этой информационной системе или в сегментах информационной системы при их наличии, масштаб информационной системы и (или) сегментов информационной системы при их наличии, присвоенный класс защищённости информационной системе или сегментам информационной системы при их наличии.

5.7. Класс защищённости информационной системы (сегментов информационной системы) подлежит пересмотру при изменении масштаба информационной системы (сегментов информационной системы) или значимости содержащейся в ней информации (в сегментах информационной системы).

5.8. Результаты классификации информационной системы (сегментов информационной системы) в обязательном порядке отражаются в перечне объектов защиты информации, утверждаемом в соответствии с пунктом 5.3 настоящей Политики.

5.9. В отношении информационных систем Учреждения, включённых в перечень, утверждённый в соответствии с пунктом 5.3 настоящей Политики, обрабатывающих персональные данные, производится определение уровня защищённости персональных данных в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утверждёнными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

5.10. Результаты определения уровня защищённости персональных данных при их обработке в информационной системе персональных данных оформляются Актом определения уровня защищённости персональных данных при их обработке в информационной системе персональных данных Учреждения, который утверждается главным врачом, или включаются в Акт классификации информационной системы.

5.11. Уровень защищённости персональных данных при их обработке в информационной системе персональных данных Учреждения подлежит пересмотру при изменении категорий персональных данных, обрабатываемых в информационной системе, типов субъектов персональных данных, чьи персональные данные обрабатываются в информационной системе, количества субъектов персональных данных в разрезе категорий персональных данных, типа угроз, актуальных для информационной системы.

6. ЛИЦА, УЧАСТВУЮЩИЕ В ЗАЩИТЕ ИНФОРМАЦИИ

6.1. В деятельности по защите информации в Учреждении участвуют следующие категории лиц: ответственный за организацию защиты информации, специалист по защите информации, пользователи, обеспечивающие эксплуатацию информационных систем, пользователи, использующие информационные системы, а также привлекаемые подрядные (в том числе специализированные) организации.

6.2. Ответственный за организацию защиты информации:

6.2.1. Организует деятельность по защите информации, управляет защитой информации и контролирует данную деятельность;

6.2.2. Создаёт (определяет) структурное подразделение, на которое возлагаются функции подразделения обеспечивающего информационную безопасность Учреждения, в том числе обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты;

6.2.3. Утверждает политику защиты информации, внутренние стандарты, регламенты и иные документы Учреждения по защите информации;

6.2.4. Выделяет необходимые организационные, материально-технические и иные ресурсы для проведения мероприятий и принятия мер по защите информации;

6.2.5. Принимает решения о необходимости привлечения дополнительных сил и средств для защиты информации, включая привлечение специализированных организаций;

6.2.6. Согласовывает планы проведения мероприятий по защите информации;

6.2.7. Принимает управленческие решения о необходимости совершенствования защиты информации, в том числе решение о необходимости разработки плана мероприятий по совершенствованию защиты информации (в случае несоответствия показателя защищённости Кзи и показателя уровня зрелости Пзи нормативным значениям, установленным в методических документах ФСТЭК России);

6.2.8. Организует непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также взаимодействие автоматизированном режиме с Центром мониторинга и управления сетью связи общего пользования;

6.2.9. Взаимодействует с ФСТЭК России, ФСБ России и иными организациями по вопросам, связанным с защитой информации, от лица Учреждения.

6.3. Специалист по защите информации:

6.3.1. Осуществляет планирование, проведение мероприятий и принятие мер по защите информации;

6.3.2. Разрабатывает и представляет ответственному за организацию защиты информации обоснованные предложения по организационным, материально-техническим и иным ресурсам, необходимым для проведения мероприятий и принятия мер по защите информации;

6.3.3. Разрабатывает и представляют на утверждение проекты документов по защите информации (стандарты, регламенты и иные внутренние документы по защите информации);

6.3.4. Готовит предложения о необходимости привлечения специализированных организаций для защиты информации;

6.3.5. Контролирует соблюдение подрядными (в том числе специализированными) организациями (при их привлечении) настоящей Политики и иных документов Учреждения по защите информации;

6.3.6. Осуществляет приёмку результатов работ и услуг, выполняемых (оказываемых) специализированными организациями;

6.3.7. Выявляет и оценивает угрозы безопасности информации;

6.3.8. Проводит периодическую оценку текущего состояния защиты информации от базового уровня угроз безопасности информации (показатель защищённости Кзи);

6.3.9. Проводит периодическую оценку достаточности и эффективности проведения мероприятий по защите информации (показатель уровня зрелости Пзи);

6.3.10. Информирует ответственного за организацию защиты информации о результатах оценки показателя защищённости Кзи и показателя уровня зрелости Пзи (в случае их несоответствия нормативным значениям, указанным в методических документах ФСТЭК России) в сроки, установленные внутренними регламентами по защите информации;

6.3.11. Направляет в ФСТЭК России результаты оценки показателя защищённости Кзи и показателя уровня зрелости Пзи в объёме и сроки, установленные внутренними регламентами по защите информации;

6.3.12. Разрабатывает план мероприятий по совершенствованию защиты информации по результатам оценки состояния защиты информации и предоставляет его ответственному за организацию защиты информации;

6.3.13. Определяет и поддерживает в актуальном состоянии перечень объектов защиты;

6.3.14. Обеспечивает непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в том числе в автоматизированном режиме с Центром мониторинга и управления сетью связи общего пользования;

6.3.15. Взаимодействует со всеми работниками Учреждения по вопросам защиты информации.

6.4. При назначении специалистов по защите информации Учреждение руководствуется следующими принципами:

– специалисты по защите информации должны обладать компетенциями, необходимыми для выполнения возлагаемых на них функций;

– не менее 30% сотрудников структурного подразделения, на которое возложены функции подразделения обеспечивающего информационную безопасность Учреждения, в том числе обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты (в случае создания (определения) такого подразделения) должны иметь профессиональное образование по специальности или направлению подготовки в области информационной безопасности или пройти обучение по программе профессиональной переподготовки в области информационной безопасности.

6.5. Пользователи, обеспечивающие эксплуатацию информационных систем:

6.5.1. Представляют специалисту по защите информации (по его запросу) актуальные данные об архитектуре, применяемых решениях, оборудовании и программном обеспечении, а также процессах и особенностях функционирования (сопровождения, обслуживания, ремонта) информационных систем;

6.5.2. Участвуют, проводят мероприятия и принимают меры по защите информации в ходе сопровождения, обслуживания информационных систем, поставки комплектующих и иных видов работ по эксплуатации информационных систем в объёме, установленном во внутренних стандартах и регламентах по защите информации;

6.5.3. Взаимодействуют со специалистом по защите информации по вопросам защиты информации.

6.6. Пользователи, использующие информационные системы:

6.6.1. Представляют специалисту по защите информации (по его запросу) актуальные данные о процессах обработки информации и особенностях эксплуатации информационных систем;

6.6.2. Принимают участие в проведении мероприятий и принятии мер по защите информации в объёме, установленном во внутренних стандартах и регламентах по защите информации;

6.6.3. Взаимодействуют со специалистом по защите информации по вопросам защиты информации.

6.7. Подрядные (в том числе специализированные) организации: соблюдают положения настоящей Политики и иных документов Учреждения в части, соответствии с условиями заключенных договоров.

7. ОРГАНИЗАЦИОННАЯ СИСТЕМА УПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТЬЮ ПО ЗАЩИТЕ ИНФОРМАЦИИ

7.1. В Учреждении действует организационная система управления деятельностью по защите информации (далее – СУЗИ), представляющая собой совокупность взаимосвязанных элементов: лиц, указанных в разделе 6 настоящей Политики, процессов и документов.

7.2. Целью СУЗИ является обеспечение достижения целей защиты информации, установленных разделом 3 настоящей Политики, посредством эффективного планирования, исполнения, контроля и постоянного совершенствования.

7.3. Ответственный за организацию защиты информации возглавляет СУЗИ и несет общую ответственность за её функционирование.

7.4. Исполнительным элементом СУЗИ является специалист по защите информации, на которого возложена практическая реализация мероприятий и мер защиты.

7.5. В СУЗИ в обязательном порядке вовлечены:

– пользователи, обеспечивающие эксплуатацию информационных систем;

– пользователи, использующие информационные системы;

– представители подрядных (в том числе специализированных) организаций, на которых возложены обязанности по соблюдению безопасной обработки информации в процессе выполнения работ и оказания услуг.

7.6. Взаимодействие между элементами СУЗИ является непрерывным и осуществляется в соответствии с настоящей Политикой, внутренними регламентами и должностными инструкциями. Схема организационной структуры и взаимодействия в системе управления защитой информации приведена в Приложении к настоящей Политике.

7.7. Управление деятельностью по защите информации осуществляется в рамках следующих ключевых процессов:

7.7.1. Планирование деятельности по защите информации.

Включает:

– определение целей защиты информации и негативных последствий (событий), наступление которых может привести к нарушению установленных целей защиты информации;

– классификацию информационных систем и определение объектов защиты (информационные системы, программные, программно-аппаратные средства, несанкционированный доступ к которым и (или) воздействие на которые могут привести к нарушению целей защиты информации);

– выявление и оценку угроз безопасности информации с использованием банка данных угроз ФСТЭК России и действующих методических документов ФСТЭК России, и ФСБ России;

– разработку и утверждение планов мероприятий и принятия мер по защите информации (планируемые мероприятия и принимаемые меры направлены на блокирование (нейтрализацию) актуальных угроз безопасности информации);

– определение и выделение необходимых обеспечивающих ресурсов мероприятий и принятия мер.

7.7.2. Исполнение (проведение мероприятий и принятие мер по защите информации).

Включает практическую реализацию всего комплекса мер защиты, предусмотренных разделом III Требований, утверждённых приказом ФСТЭК России от 11 апреля 2025 г. № 117, настоящей Политикой, проектной и рабочей документацией на систему защиты информации.

7.7.3. Контроль и оценка эффективности.

Включает:

– мониторинг информационной безопасности;

– регулярную оценку состояния защиты информации от базового уровня угроз безопасности информации (показателя Кзи) - не реже 1 раза в 6 месяцев;

– регулярную оценку зрелости процессов защиты информации (показателя Пзи) – не реже 1 раза в 2 года;

– регулярный контроль уровня защищённости информации (анализ уязвимостей, проведение аудитов, тестов на проникновение и др.);

– представление отчётности о результатах оценки в ФСТЭК России в установленные сроки.

7.7.4. Совершенствование (корректирующие и предупреждающие действия).

Включает:

– анализ результатов контроля уровня защиты информации и результатов оценок показателей Кзи и Пзи;

– разработку и утверждение планов мероприятий по совершенствованию защиты информации, направленных на достижение нормативных значений показателей Кзи и Пзи (по решению ответственного за организацию защиты информации);

– внедрение корректирующих мер и актуализацию внутренних документов Учреждения по защите информации.

7.8. Процессы, указанные в пункте 7.7 настоящей Политики, образуют цикл непрерывного улучшения (Plan-Do-Check-Act, PDCA), обеспечивающий постоянное развитие и адаптацию системы защиты информации к изменениям в угрозах безопасности информации, технологиях и деятельности Учреждения.

7.9. Каждый цикл завершается анализом результативности СУЗИ и планированием действий для следующего цикла.

7.10. Неотъемлемой частью СУЗИ является документирование её деятельности. Основу документального подтверждения функционирования СУЗИ составляют следующие документы:

– настоящая Политика защиты информации;

– внутренние стандарты и регламенты по защите информации;

– перечень объектов защиты информации;

– планы мероприятий и принятия мер по защите информации;

– модели угроз безопасности информации.

7.11. Деятельность СУЗИ отражается в отчётных и рабочих документах, таких как акты классификации информационных систем, акты оценок показателей Кзи и Пзи отчёты о проведённых мероприятиях и принятых мерах, протоколы, журналы и иные документы.

8. ОТВЕТСТВЕННОСТЬ

8.1. Несоблюдение требований настоящей Политики, внутренних стандартов, регламентов и иных документов Учреждения в области защиты информации влечёт за собой ответственность в соответствии с законодательством Российской Федерации и внутренними документами Учреждения.

8.2. Ответственный за организацию защиты информации несёт персональную ответственность за организацию деятельности по защите информации, выделение и целевое использование ресурсов, результаты оценки показателей Кзи и Пзи и соблюдение запретов, установленных законодательством Российской Федерации в отношении применения средств защиты информации.

8.3. Специалист по защите информации несёт персональную ответственность за неисполнение или ненадлежащее исполнение обязанностей, установленных разделом 6 настоящей Политики, его должностными инструкциями, внутренними стандартами и регламентами по защите информации, в частности, за непринятие установленных мер по выявлению угроз, управлению уязвимостями, мониторингу информационной безопасности, оценке состояния защиты (показателей Кзи и Пзи) и контролю за подрядными организациями, если такие действия (бездействие) привели или могли привести к нарушению целей защиты информации.

8.4. Руководители подразделений Учреждения несут ответственность за соблюдение подчинёнными им сотрудниками требований по защите информации, а также за своевременное и полное взаимодействие подчинённых им сотрудников со специалистом по защите информации.

8.5. Сотрудники Учреждения, обеспечивающие эксплуатацию информационных систем, несут ответственность за корректную реализацию технических мер защиты в рамках своих должностных обязанностей, своевременное устранение выявленных уязвимостей и информирование специалиста по защите информации о возникающих рисках.

8.6. Пользователи информационной системы Учреждения (сотрудники Учреждения) несут персональную ответственность за:

– соблюдение установленных правил доступа и работы с информацией;

– сохранность средств аутентификации (паролей, электронных ключевых носителей);

– своевременное информирование специалиста по защите информации о подозрительных событиях или возможных инцидентах.

8.7. Подрядные (в том числе специализированные) организации несут ответственность за выполнение взятых на себя обязательств по защите информации в соответствии с условиями заключенных договоров. Нарушение ими требований настоящей Политики является основанием для применения мер ответственности, предусмотренных договором.

8.8. Факты нарушения требований защиты информации подлежат обязательному расследованию комиссией, назначаемой локальным актом Учреждения, для причин, обстоятельств и определения мер ответственности.

ПРИЛОЖЕНИЕ
к Политике защиты информации в бюджетном учреждении здравоохранения Удмуртской Республики «Республиканская офтальмологическая клиническая больница Министерства здравоохранения Удмуртской республики»

Схема организационной структуры и взаимодействия в системе управления защитой информации