ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ ГОРОДА МОСКВЫ
«ПСИХИАТРИЧЕСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА № 1 им. Н.А. АЛЕКСЕЕВА ДЕПАРТАМЕНТА ЗДРАВООХРАНЕНИЯ ГОРОДА МОСКВЫ»

Приложение 2
к приказу ГБУЗ «ПКБ № 1 ДЗМ»
от 31.01.2024 № 75

Политика информационной безопасности

ГБУЗ «ПКБ № 1 ДЗМ»

Москва 2024

Общие положения.

Политика информационной безопасности (далее – Политика) ГБУЗ «ПКБ № 1 ДЗМ» (далее - Учреждение) определяет систему взглядов на проблему обеспечения информационной безопасности (далее - ИБ) и определяет мероприятия, процедуры и правила по защите информации.

Положения настоящей Политики обязательны к исполнению для всех сотрудников Учреждения.

В Учреждении защите подлежит информация, которая в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» является информацией, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Целями настоящей Политики являются:

– обеспечение безопасности объектов защиты Учреждения от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности информации;

– нейтрализация актуальных угроз безопасности информации;

– выполнение требований действующего законодательства по защите информации.

В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.

Настоящая Политика разработана с учетом положений следующих законодательных и нормативно-правовых актов:

– Конституция Российской Федерации;

– Гражданский и Уголовный кодексы;

– Кодекс об административных правонарушениях;

– законы, указы, постановления и другие нормативные документы действующего законодательства Российской Федерации;

– нормативные документы федерального и территориальных фондов обязательного медицинского страхования, министерств здравоохранения и социального развития, департамента здравоохранения Москвы, Федеральной службы страхового надзора и др.;

– нормативные и регламентирующие документы государственных органов Российской Федерации (ФСТЭК, ФСБ, Роскомнадзор и др.);

– внутренние нормативно-методические и организационно-распорядительные документы Учреждения.

Объекты защиты.

В Учреждении должны быть выявлены и оценены с точки зрения их важности все ресурсы. Для всех ценных ресурсов должен быть составлен реестр (перечень). В соответствии с реестром (перечнем) о ресурсах Учреждения реализуется защита информации, степень которой соразмерна ценности и важности ресурсов.

В Учреждении имеются следующие типы ресурсов:

– информационные ресурсы с ограниченным доступом, составляющие врачебную тайну, персональные данные, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, в том числе открытая (общедоступная) информация, представленные в виде документов и массивов информации, независимо от формы и вида их представления;

– информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Оценка рисков.

В Учреждении должны быть определены требования к безопасности путем методической оценки рисков. Оценки рисков должны выявить, определить количество и расположить по приоритетам риски в соответствии с критериями принятия рисков и целями Учреждения.

Оценка рисков предполагает системное сочетание анализа рисков и оценивания рисков.

Кроме того, оценка рисков и выбор механизмов контроля должны производиться периодически, чтобы:

– учесть изменения требований и приоритетов;

– принять во внимание новые угрозы и уязвимости;

– убедиться в том, что реализованные средства сохранили свою эффективность.

Перед обработкой каждого риска Учреждение должно выбрать критерии для определения возможности принятия этого риска. Риск может быть принят, если его величина достаточно мала и стоимость обработки нерентабельна для Учреждения. Такие решения должны регистрироваться.

Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

– применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня;

– сознательное и объективное принятие риска, если он точно удовлетворяет Политике Учреждения и критериям принятия рисков;

– уклонение от риска путем недопущения действий, могущих быть его причиной;

– передача рисков другой стороне (аутсорсинг, страхование и т.п.).

Меры и средства обеспечения информационной безопасности.

В Учреждении необходимо выделить следующие основные меры обеспечения информационной безопасности:

– законодательные (законодательство Российской Федерации в сфере информационной безопасности);
– морально-этические (нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе);
– технологические (технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения работниками ошибок и нарушений в рамках предоставленных им прав и полномочий);
– организационные (меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность работников, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации);
– физические (меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для предотвращения несанкционированного доступа к объектам защиты, а также технических средств визуального наблюдения, связи и охранной сигнализации);
– технические (меры защиты основаны на использовании различных электронных устройств и специального программного обеспечения, выполняющих функции защиты).

Для обеспечения информационной безопасности необходимо использовать средства:

– физической защиты (введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки информации ограниченного доступа, оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи);
– антивирусной защиты (предотвращение потерь, ошибок и модификации информационных ресурсов);
– резервирования (поддержание целостности и доступности объектов защиты);
– разграничения доступа (управление доступом к информационным ресурсам, к сети общего пользования, к локальной вычислительной сети);

– криптографической защиты (защита конфиденциальности, целостности и аутентичности информационных ресурсов путем применения средств криптографической защиты информации, в том числе при передаче по каналам связи);

– идентификации и аутентификации (предотвращение работы с информационными ресурсами посторонних лиц путем обеспечения возможности распознавания каждого легального пользователя);

– контроля целостности (своевременное обнаружение модификации или искажения информационных ресурсов, обеспечение правильности функционирования системы защиты и целостности хранимой и обрабатываемой информации);

– мониторинга событий информационной безопасности (обеспечение обнаружения и регистрации всех событий, которые могут повлечь за собой нарушение информационной безопасности).

Безопасность персонала.

Роли и обязанности по обеспечению безопасности информационных ресурсов, описанные в соответствии с Политикой, должны быть доведены до сведения работника при трудоустройстве.

Условия найма.

Все принимаемые на работу сотрудники должны одобрить и подписать свои трудовые договоры, в которых устанавливается их ответственность за информационную безопасность. В договор должно быть включено согласие работника на проведение контрольных мероприятий со стороны Учреждения по проверке выполнения требований информационной безопасности, а также обязательства по неразглашению информации ограниченного доступа. В договоре должны быть описаны меры, которые будут приняты в случае несоблюдения работником требований информационной безопасности.

Обязанности по соблюдению мер информационной безопасности должны быть включены в должностные инструкции каждого работника Учреждения.

Все принимаемые работники должны быть ознакомлены под подпись с перечнем информации ограниченного доступа, с установленным режимом с ней и с мерами ответственности за нарушение этого режима.

При предоставлении работнику доступа к информационным системам Учреждения он должен ознакомиться под подпись с инструкцией пользователя информационной системы и инструкцией по обеспечению безопасности информационной системы.

Обучение информационной безопасности.

Все работники должны проходить периодическую подготовку в области политики и процедур информационной безопасности, принятых в Учреждении.

Завершение или изменения трудовых отношений.

При увольнении все предоставленные работнику права доступа к ресурсам информационных систем должны быть удалены. При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых отношениях.

Защищенные области.

Средства обработки информации, поддерживающие критически важные и уязвимые ресурсы Учреждения, должны быть размещены в защищенных областях. Такими средствами являются: серверы, магистральное телекоммуникационное оборудование, телефонные станции, кроссовые панели, оборудование, обеспечивающее обработку и хранение сведений конфиденциального характера.

Защищенные области должны обеспечиваться соответствующими средствами контроля доступа, обеспечивающим возможность доступа только авторизованного персонала.

Области общего доступа.

Места доступа, через которые неавторизованные лица могут попасть в помещения Учреждения, должны контролироваться и, если это возможно, должны быть изолированы от средств обработки информации с целью предотвращения несанкционированного доступа.

Вспомогательные службы.

Все вспомогательные службы, такие как электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха должны обеспечивать гарантированную и устойчивую работоспособность компонентов информационных систем Учреждения.

Утилизация или повторное использование оборудования.

Со всех носителей информации, которыми укомплектовано утилизируемое оборудование, должны гарантированно удаляться все данные ограниченного доступа и лицензионное программное обеспечение.

Перемещение имущества.

Оборудование, информация или программное обеспечение должны перемещаться за пределы Учреждения только при наличии письменного разрешения начальника Технического отдела. Работники, имеющие право перемещать оборудование и носители информации за пределы Учреждения должны быть четко определены. Время перемещения оборудования за пределы Учреждения и время его возврата должны регистрироваться.

Контроль доступа.

Основными пользователями информации в информационной системе Учреждения являются работники структурных подразделений. Уровень полномочий каждого пользователя определяется индивидуально. Каждый работник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями.

Допуск пользователей к работе с информационными ресурсами должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться в установленном порядке, согласно регламента предоставления доступа пользователей.

Управление привилегиями.

Доступ работника к информационным ресурсам Учреждения должен быть санкционирован руководителем структурного подразделения, в котором числится согласно штатному расписанию данный работник, и владельцами соответствующих информационных ресурсов. Управление доступом осуществляется в соответствии с установленными процедурами.

Наделение привилегиями и их использование должно быть строго ограниченным и управляемым. Распределение привилегий должно управляться с помощью процесса регистрации этих привилегий.

Контроль и периодический пересмотр прав доступа пользователей к информационным ресурсам Учреждения осуществляется в процессе аудита информационной безопасности в соответствии с правилами аудита информационной безопасности и установленными процедурами.

Управление паролями.

Пароли – средство проверки личности пользователя для доступа к информационной системе или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

Предоставление паролей должно контролироваться посредством официальной процедуры и в соответствии с нормативно-правовыми актами Учреждения.

При необходимости возможно использование других технологий идентификации и аутентификации пользователей, в частности, биометрических технологий, проверки подписи и аппаратных средств (смарт-карты, e-Token/ruToken, чипы и т.п.).

Контроль прав доступа.

Чтобы обеспечить эффективный контроль доступа, необходимо ввести официальный процесс регулярной проверки прав доступа пользователей.

Использование паролей.

Идентификатор и пароль пользователя в информационной системе являются учетными данными, на основании которых работнику Учреждения предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой и хранимой) работником информации.

Не допускается использование различными пользователями одних и тех же учетных данных.

Учреждение оставляет за собой право:

– осуществлять периодическую проверку стойкости паролей пользователей, используемых работниками для доступа к информационным системам;

– принимать меры дисциплинарного характера к сотрудникам, нарушающим положения настоящей Политики.

Политика чистого стола.

Работники Учреждения обязаны:

– сохранять известные им пароли в тайне;

– закрывать активные сеансы по завершении работы, если только их нельзя защитить подходящим блокирующим механизмом, например, защищенный паролем хранитель экрана;

– по завершении сеанса выходить из системы универсальных ЭВМ, серверов и офисных ПК.

Запрещается вести запись паролей (например, на бумаге, в программном файле или в карманном устройстве), за исключением случаев, когда запись может храниться безопасно, а метод хранения был утвержден.

Документы и носители с информацией ограниченного доступа должны убираться в запираемые места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места.

Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы, когда они находятся без присмотра.

Документы, содержащие информацию ограниченного доступа, должны изыматься из печатающих устройств немедленно.

В конце рабочего дня работник должен привести в порядок письменный стол и убрать все офисные документы в запираемый шкаф или сейф.

Для утилизации документов, содержащих информацию ограниченного доступа, должны использоваться уничтожители бумаги.

По окончании рабочего дня и в случае длительного отсутствия на рабочем месте необходимо запирать на замок все шкафы и сейфы.

Мобильное компьютерное оборудование.

При использовании мобильных устройств (например, ноутбуков, планшетов и мобильных телефонов) необходимо соблюдать особые меры предосторожности, чтобы не допустить компрометацию информации, принадлежащей Учреждению.

Под использованием мобильных устройств и носителей информации в информационных системах Учреждения понимается их подключение к инфраструктуре информационных систем с целью обработки, приема/передачи информации между информационной системой и мобильными устройствами, а также носителями информации.

На предоставленных Учреждением мобильных устройствах допускается использование программного обеспечения, входящего в Перечень разрешенного к использованию программного обеспечения.

К предоставленным Учреждением мобильным устройствам и носителям информации предъявляются те же требования информационной безопасности, что и для стационарных автоматизированных рабочих мест. Целесообразность дополнительных мер обеспечения информационной безопасности определяется работником, ответственным за информационную безопасность.

Политика допустимого использования информационных ресурсов.

Использование программного обеспечения.

На автоматизированных рабочих местах Учреждения допускается использование только лицензионного программного обеспечения, утвержденного в Перечне разрешенного к использованию программного обеспечения.

Использование автоматизированных рабочих мест и информационных систем.

К работе в информационной системе Учреждения допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам информационной безопасности.

Использование ресурсов локальной сети.

Для выполнения своих должностных обязанностей каждый работник обеспечивается доступом к соответствующим информационным ресурсам. Информационными ресурсами являются каталоги и файлы, хранящиеся на дисках серверов Учреждения, базы данных, электронная почта.

Основными рабочими каталогами являются личные каталоги работников и каталоги подразделений, созданные в соответствии с особенностями их работы. Доступ работников к ресурсам сети осуществляется согласно матрицы доступа.

Обработка информации ограниченного доступа.

При обработке информации ограниченного доступа работники обязаны соблюдать положения инструкций по работе с такой информацией.

Для выполнения должностных обязанностей работники Учреждения обязаны использовать адреса электронной почты, зарегистрированные в почтовом домене Департамента здравоохранения города Москвы zdrav.mos.ru, запрещается использование сторонних сервисов электронной почты.

Работа в сети.

Должны быть реализованы меры для обеспечения безопасности информации в сетях и защиты подключенных сервисов от несанкционированного доступа в том числе с использованием шлюзов безопасности, предназначенных для построения виртуальной сети и обеспечения безопасной передачи данных между ее защищенными сегментами, а также фильтрации IP-трафика.

Доступ к сети Интернет предоставляется работникам Учреждения в целях выполнения ими своих должностных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

Для доступа работников Учреждения к сети Интернет допускается применение программного обеспечения, входящего в Перечень разрешенного к использованию программного обеспечения.

Учреждение оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению должностных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством.

Приобретение, разработка и обслуживание систем.

Требования безопасности для информационных систем.

При описании требований к созданию новых систем или к усовершенствованию существующих необходимо учитывать потребность в средствах обеспечения безопасности.

Требования к безопасности и средства защиты должны соответствовать ценности используемых информационных ресурсов и потенциальному ущербу для Учреждения в случае сбоя или нарушения безопасности. Основой для анализа требований к безопасности и выбору мер для поддержки безопасности является оценка рисков и управление рисками.

Системные требования к информационной безопасности и процессам, обеспечивающим защиту информации, должны быть включены на ранних стадиях проектирования информационных систем.

Защита от вредоносных программ.

Защита должна основываться на применении программного обеспечения для обнаружения вредоносных программ и восстановления данных, осведомленности об информационной безопасности, соответствующих мерах контроля доступа к системе и управлению изменениями. Должны быть обеспечены следующие меры:

– проверка любых файлов, полученных по сети или через любой другой носитель, на наличие вредоносных программ перед использованием;

– проверка вложений и загружаемых файлов электронной почты на наличие вредоносных программ перед использованием, такое сканирование должно проводиться в разных местах, например, на серверах, настольных компьютерах и на первой линии сети Учреждения.

Безопасность системных файлов.

Чтобы свести к минимуму риск повреждения информационных систем, в Учреждении необходимо обеспечить контроль над внедрением программного обеспечения в рабочих системах.

Безопасность процесса разработки и обслуживания систем.

Чтобы свести к минимуму вероятность повреждения ИС Учреждения, следует ввести строгий контроль над внесением изменений. Необходимо установить официальные правила внесения изменений. Эти правила должны гарантировать, что процедуры, связанные с безопасностью и контролем, не будут нарушены, что программисты, занимающиеся поддержкой, получат доступ только к тем частям системы, которые необходимы для их работы, и что

для выполнения любого изменения требуется получить официальное разрешение и подтверждение.

Тестовые данные должны находиться под контролем и защитой. Необходимо избегать использования рабочих баз данных, содержащих информацию ограниченного доступа. Если эти базы все же будут использоваться, то информация ограниченного доступа должна быть удалена или обезличена.

После внесения изменений в информационную систему, критичные для информационных процессов Учреждения приложения должны анализироваться и тестироваться, чтобы гарантировать отсутствие вредных последствий для безопасности Учреждения.

Криптографические средства.

Все поступающие в Учреждение средства криптографической защиты должны быть учтены в соответствующем журнале поэкземплярного учета СКЗИ.

В Учреждении должно осуществляться управление ключами для эффективного применения криптографических методов. Компрометация или потеря криптографических ключей может привести к нарушению конфиденциальности, подлинности и/или целостности информации.

Все ключи должны быть защищены от изменения, утери и уничтожения. Кроме того, секретные и закрытые ключи должны быть защищены от несанкционированного доступа. Оборудование, используемое для генерации, хранения и архивирования ключей должно быть физически защищено.

Соглашения с внешними поставщиками криптографических услуг (например, удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надежности сервиса и времени реакции при предоставлении сервиса.

Криптографические системы и методы следует использовать для защиты информации ограниченного доступа, когда другие средства контроля не обеспечивают адекватной защиты.

Для критической информации должно использоваться шифрование при их хранении в базах данных или передаче по коммерческим или открытым сетям, таким как Интернет. Шифрование любой другой информации в информационных системах Учреждения должно осуществляться только после получения письменного разрешения на это.

При использовании шифрования в информационных системах Учреждения должны применяться только утвержденные стандартные алгоритмы и сертифицированные ФСБ России продукты, их реализующие.

Электронная подпись.

Электронная подпись обеспечивают защиту аутентификации и целостности электронных документов.

Электронные подписи могут применяться для любой формы документа, обрабатываемого электронным способом. Электронные подписи должны быть реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой – для проверки подписи (открытый ключ).

Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой, имеющий к нему доступ, может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Защиты целостности открытого ключа должна обеспечиваться при использовании сертификата открытого ключа.

Криптографические ключи, используемые для цифровых подписей, должны отличаться от тех, которые используются для шифрования.

При использовании электронной подписи, необходимо учитывать требования действующего законодательства Российской Федерации, определяющего условия, при которых цифровая подпись имеет юридическую силу.

Управление ключами.

Управление криптографическими ключами важно для эффективного использования криптографических средств.

Любая компрометация или потеря криптографических ключей может привести к компрометации конфиденциальности, подлинности и/или целостности информации. Следует применять систему защиты для обеспечения использования в информационных системах Учреждения криптографических методов в отношении открытых ключей, где каждый пользователь имеет пару ключей, открытый ключ (который может быть показан любому) и личный ключ (который должен храниться в секрете). Методы с открытыми ключами должны использоваться для шифрования и для генерации электронных подписей.

Ключи необходимо защищать от изменения и разрушения, а секретным и личным ключам необходима защита от неавторизованного раскрытия. Криптографические методы могут также использоваться для этой цели. Физическую защиту следует применять для защиты оборудования, используемого для изготовления, хранения и архивирования ключей.

Секретные ключи пользователей должны храниться так же, как и пароли. О любом подозрении на компрометацию секретного ключа пользователь должен немедленно сообщить работнику, ответственному за информационную безопасность в Учреждении.

Соглашения с внешними поставщиками криптографических услуг (например, с удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надежности сервиса и времени реакции при предоставлении сервиса.

Управление инцидентами информационной безопасности.

В Учреждении разработана и утверждена процедура уведомления о происшествиях в области информационной безопасности, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться при поступлении сообщений о происшествии.

Все работники должны быть ознакомлены с процедурой уведомления, а в их обязанности должна входить максимально быстрая передача информации о происшествиях.

В дополнение к уведомлению о происшествиях информационной безопасности и недостатках безопасности должен использоваться мониторинг систем, сообщений и уязвимостей для обнаружения инцидентов информационной безопасности.

Цели управления инцидентами информационной безопасности должны быть согласованы с главным врачом для учета приоритетов Учреждения при обращении с инцидентами.

Необходимо создать механизмы, позволяющие оценивать и отслеживать типы инцидентов, их масштаб и связанные с ними затраты.

Управление непрерывностью и восстановлением.

Необходимо разработать контролируемый процесс для обеспечения и поддержки непрерывности деятельности Учреждения. Данный процесс должен объединять в себе основные элементы поддержки непрерывности деятельности.

В Учреждении должны быть разработаны и реализованы планы, которые позволят продолжить или восстановить операции и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя критически важных процессов Учреждения.

В каждом плане поддержки непрерывности рабочих процессов Учреждения должны быть четко указаны условия начала его исполнения и работники, ответственные за выполнение каждого фрагмента плана. При появлении новых требований необходимо внести поправки в принятые планы действия в нештатных ситуациях.

Для каждого плана должен быть назначен определенный владелец. Правила действия в нештатных ситуациях, планы ручного аварийного восстановления и планы возобновления деятельности должны находиться в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение.

Соблюдение требований законодательства.

Все значимые требования, установленные действующим законодательством, подзаконными актами и договорными отношениями, а также подход Учреждения к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии.

Необходимо соблюдение регламентированного процесса, предупреждающего нарушение целостности, достоверности и конфиденциальности информационных ресурсов, содержащих информацию ограниченного доступа, начиная от стадии сбора и ввода данных до их хранения.

Важная документация Учреждения должна быть защищена от утери, уничтожения и фальсификации в соответствии с требованиями законодательства и подзаконных актов.

Система хранения и обработки должна обеспечивать четкую идентификацию записей и их периода хранения в соответствии с требованиями законов и нормативных актов. Эта система должна иметь возможность уничтожения записей по истечении периода хранения, если эти записи больше не требуются Учреждению.

Криптографические средства должны использоваться в соответствии со всеми имеющимися соглашениями, законодательными и нормативными актами.

Аудит информационной безопасности.

Учреждение должно проводить внутренние проверки системы управления информационной безопасностью через запланированные интервалы времени.

Руководство и работники Учреждения при проведении у них аудита системы управления информационной безопасностью обязаны оказывать содействие аудиторам и предоставлять всю необходимую для проведения аудита информацию.

Контроль и пересмотр.

Работник, ответственный за информационную безопасность в Учреждении, ежегодно пересматривает положения настоящей политики. Изменения и дополнения утверждаются главным врачом.

Все изменения, внесенные в настоящую Политику должны учитываться в листе «История изменений».

История изменений

Версия	Дата утверждения	Изменения	Кто внес изменения