Утверждено
Приказом от __.__.2017 № _____

ПОЛИТИКА
негосударственного учреждения здравоохранения «Отделенческая больница на станции Муром открытого акционерного общества «Российские железные дороги» в отношении обработки персональных данных

1. Термины и определения

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

Обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники.

Распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Назначение и правовая основа документа

Политика негосударственного учреждения здравоохранения «Отделенческая больница на станции Муром открытого акционерного общества «Российские железные дороги» (далее по тексту – Больница) определяет систему взглядов на проблему обеспечения безопасности ПДн и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется Больница в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности ПДн.

Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский, Уголовный и Трудовой кодексы, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы ФСТЭК и ФСБ России.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности ПДн Больница позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

3. Основными объектами системы безопасности ПДн в Больнице являются:

– информационные ресурсы с ограниченным доступом, содержащие ПДн;

– процессы обработки ПДн в ИСПДн Больницы, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;

– информационная инфраструктура, включающая 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 расположены технические средства обработки ПДн.

4. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении безопасности ПДн Больницы являются:

– Больница, как собственник информационных ресурсов;

– руководство и сотрудники Больницы, в соответствии с возложенными на них функциями;

– физические лица, не являющиеся сотрудниками Больницы, но имеющими с ней отношения (пациенты).

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

– своевременного доступа к необходимым им ПДн (их доступности);
– достоверности (полноты, точности, адекватности, целостности) ПДн;
– конфиденциальности (сохранения в тайне) ПДн;
– защиты от навязывания им ложных (недостоверных, искаженных) ПДн;
– разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с ПДн;
– возможности осуществления непрерывного контроля и управления процессами обработки и передачи ПДн;
– защиты ПДн от незаконного распространения.

4.1. Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Больницы от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на ПДн, их носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств ПДн:

– доступности для легальных пользователей (устойчивого функционирования информационных систем Больницы, при котором пользователи имеют возможность получения необходимых ПДн и результатов решения задач за приемлемое для них время);
– целостности и аутентичности (подтверждение авторства) ПДн, хранимых и обрабатываемых в информационных системах Больницы и передаваемой по каналам связи;
– конфиденциальности - сохранения в тайне определенной части ПДн, хранимых, обрабатываемых и передаваемых по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности ПДн обеспечивается соответствующими множеству значимых угроз методами и средствами.

4.2. Основные задачи системы обеспечения безопасности ПДн

Для достижения основной цели защиты и обеспечения указанных свойств ПДн система обеспечения информационной безопасности Больницы должна обеспечивать эффективное решение следующих задач:

– своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем Больницы;
– создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

– создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

– защиту от вмешательства в процесс функционирования информационных систем посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

– разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Больницы (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;

– обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

– защиту от несанкционированной модификации используемых в информационных системах Больницы программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

– защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

4.3. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

– строгим учетом всех подлежащих защите ресурсов информационных систем Больницы (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

– журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационных систем;

– полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Больницы по вопросам обеспечения безопасности информации;

– подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности ПДн и процессов их обработки;

– наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Больницы;

– четким знанием и строгим соблюдением всеми пользователями информационных систем Больницы требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

– персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Больницы;

– непрерывным поддержанием необходимого уровня защищенности элементов информационной среды;

– применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

– эффективным контролем над соблюдением пользователями информационных ресурсов требований по обеспечению безопасности информации;

– юридической защитой интересов Больницы при взаимодействии с внешними организациями (связанном с обменом ПДн) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

5. Построение системы, обеспечения безопасности ПДн Больницы, и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

5.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности ПДн Больницы в соответствии с действующим законодательством в области защиты ПДн, а также других законодательных актов по безопасности информации РФ, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с ПДн. Принятые меры безопасности ПДн не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

Все пользователи ИСПДн должны иметь представление об ответственности за правонарушения в области обработки ПДн.

5.2. Системность

Системный подход к построению системы защиты информации в Больнице предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места ИСПДн, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников).

Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.3. Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

5.4. Непрерывность защиты

Обеспечение безопасности ПДн - процесс, осуществляемый руководством Больницы, ответственными за организацию обработки ПДн и сотрудниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри Больницы и каждый сотрудник должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности Больницы. И ее эффективность зависит от участия руководства Больницы в обеспечении информационной безопасности ПДн.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления защиты.

5.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки информационных систем в целом и их систем защиты, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самих защищаемых информационных систем. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

5.6. Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты ПДн на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем Больницы и системы их защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

5.7. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности ПДн ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов ИСПДн Больницы. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока ПДн находятся в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть

любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

5.8. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

5.9. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

5.10. Исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования ПДн и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками или подразделениями Больницы. Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции, с тем, чтобы они не имели возможности скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

5.11. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе Больницы. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственного за обработку ПДн.

Важным элементом эффективной системы обеспечения безопасности ПДн в Больнице является высокая культура работы с информацией. Руководство Больницы несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности Больницы. Все сотрудники Больницы должны понимать свою роль в процессе обеспечения

информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

5.12. Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Больницей своей деятельности. В число таких изменений входят:

– изменения организационной и штатной структуры Больницы;

– изменение существующих или внедрение принципиально новых информационных систем;

– новые технические средства.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

5.13. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

5.14. Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

5.15. Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты ПДн должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности ПДн.

5.16. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты ПДн специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Больницы (ответственных за организацию обработки ПДн).

5.17. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности ПДн, на основе используемых систем и средств защиты ПДн, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Кроме того, эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками Больницы должны немедленно доводиться до сведения руководителя Больницы и оперативно устраняться. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

6. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности ИСПДн Больницы подразделяются на:

6.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом ИСПДн Больницы.

6.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или Больницы в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе.

6.3. Технологические меры защиты

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и

направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

6.4. Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки ПДн, использование ее ресурсов, деятельность обслуживающего персонала, 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.

6.5. Формирование политики безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности ПДн (отражающую подходы к защите ПДн) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности ПДн в Больнице целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность Больницы в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности ПДн и детализирует (регламентирует) эти правила:

– каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн;

– кто имеет права доступа к ПДн, кто и при каких условиях может читать и модифицировать ПДн и т.д.

Политика нижнего уровня должна:

– предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;

– определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к ПДн;

– выбирать программно-технические (аппаратные) средства противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

6.6. Регламентация доступа в помещения

Компоненты информационных систем Больницы должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых

ресурсов (документов, АРМ и т.п.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

Все посторонние лица допускаются в помещения с компонентами информационной системы только в присутствии сотрудников Больницы.

По окончании рабочего дня, помещения, в которых размещаются компоненты информационных систем Больницы, должны запираться на ключ, по возможности опечатываться.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

6.7. Регламентация допуска сотрудников к использованию информационных ресурсов

В рамках разрешительной системы (матрицы) доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационными системами Больницы и доступ к их ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

– каждый сотрудник пользуется только предписанными ему правами по отношению к ПДн, с которыми ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с ответственным за организацию обработки ПДн;

– руководитель Больницы имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями.

Все сотрудники Больницы и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки ПДн, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению ПДн Больницы.

Обработка ПДн в компонентах ИСПДн Больницы должна производиться в соответствии с утвержденными технологическими инструкциями.

6.8. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников Больницы, с которых возможен доступ к ресурсам информационной системы,

должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

В компонентах информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

6.9. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

Оборудование информационных систем, используемое для доступа и хранения ПДн, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться.

6.10. Подбор и подготовка персонала, обучение пользователей

Пользователи ИСПДн Больницы, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки ПДн в Больнице.

Обеспечение безопасности ПДн возможно только после выработки у пользователей определенной культуры работы, т.е. норм, обязательных для исполнения всеми, кто работает с информационными ресурсами Больницы. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов ИСПДн Больницы, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, владельцев или собственников.

Все пользователи ИСПДн Больницы должны быть ознакомлены с организационно - распорядительными документами по обеспечению безопасности ПДн Больницы, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности ПДн. Доведение требований указанных документов до лиц, допущенных к обработке защищаемых ПДн, должно осуществляться под роспись.

6.11. Ответственность за нарушения установленного порядка пользования ресурсами информационной системы

Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с ПДн, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства Больницы.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

– индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Username), на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;

– проверка подлинности пользователей (аутентификация) на основе паролей;

– реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

6.12. Средства обеспечения безопасности ПДн

Для обеспечения информационной безопасности Больницы используются следующие средства защиты:

Физические средства защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемым ПДн, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Для обеспечения физической безопасности компонентов ИСПДн необходимо осуществлять ряд организационных и технических мероприятий, включающих: проверку оборудования, предназначенного для обработки ПДн, на:

– наличие специально внедренных закладных устройств;

– введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки ПДн;

– оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

Технические средства защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности ПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

– средства разграничения доступа к данным;

– средства регистрации доступа к компонентам информационной системы и контроля за использованием информации;

– средства реагирования на нарушения режима информационной безопасности.

На технические средства защиты возлагается решение следующих основных задач:

– идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств (Advantor, Touch Memory, Smart Card и т.п.);

– регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;

– защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;

– регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

– защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.

Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами ИСПДн Больницы посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

– путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);

– путем проверки знания ими паролей;

– путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

Средства разграничения доступа

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

– на контролируемую территорию;

– в отдельные помещения;

– к компонентам информационной среды Больницы и элементам системы защиты ПДн (физический доступ);

– к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);

– к активным ресурсам (прикладным программам, задачам и т.п.);

– к операционной системе, системным программам и программам защиты.

Средства обеспечения и контроля целостности

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов систем предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации ПДн должен обеспечиваться:

– средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);

– средствами электронной подписи;

– средствами подсчета контрольных сумм (для используемого программного обеспечения).

Средства оперативного контроля и регистрации событий безопасности

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

– ведения и анализа журналов регистрации событий безопасности (системных журналов);
– получения твердой копии (печати) журнала регистрации событий безопасности;
– упорядочения журналов, а также установления ограничений на срок их хранения;
– оперативного оповещения ответственного за организацию обработки ПДн о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

– дата и время события;
– идентификатор субъекта, осуществляющего регистрируемое действие;
– действие (тип доступа).

6.13. Контроль эффективности системы защиты

Контроль эффективности защиты ПДн осуществляется с целью своевременного выявления и предотвращения утечки ПДн за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение ПДн, разрушение средств информатизации. Контроль может проводиться привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.