Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Политика информационной безопасности**

**поликлиники**

Студент: Бобрович Г.С.

ФИТ 3 курс 7 группа

Преподаватель: Савельева М.Г.

Минск 2023

# **Обоснование актуальности, цели и задачи разработки ПИБ в поликлинике**

В современном обществе главным ресурсом является информация. Информационные технологии нашли применение практические во всех сферах человеческой жизни. Компьютеры обеспечивают хранение информации, ее обработку и предоставление потребителям, реализуя таким образом информационные технологии.

Основными функциями современных информационных технологий являются:

* поиск необходимой информации и хранение;
* создание новой актуальной информации;
* решение оптимизационных задач.

При этом основной задачей является не только автоматизация трудоемких процессов обработки большого количества данных, но и получение качественно новой информации в результате обработки этих данных. Однако именно высокая степень автоматизации порождает риск снижения безопасности.

Проблема уязвимости сетей очень актуальна на сегодняшний день. Дело в том, что любой сайт содержит различные вещи, которые не видны человеческому глазу. Таким образом, эти страницы образуют своеобразную цель, по которой всевозможные вирусы (вредоносные программы) и попадают в компьютер.

Но наиболее серьезная проблема – использование вредоносных программ государственными структурами разных стран мира (так называемое кибероружие). Цели использования кибероружия могут быть самыми разными: шпионаж, уничтожение каких-либо важных информационных данных, нанесение ущерба, месть и т.д.

Еще одна важная проблема области информационных технологий – проблема незащищенности данных. На сегодняшний день информация рассматривается как товар, и этот товар очень легко украсть, модифицировать или уничтожить.

Можно сделать вывод, что на сегодняшний день информационные технологии в нашей стране развивает в неблагоприятных условиях, к которым относятся:

* несовершенство существующей системы налогообложения стало причиной слишком высоких налогов для производителей ПО;
* недостаток использования информационно-коммуникативных технологий в социальной и экономической сферах, а также на уровне государственного управления;
* наличие неравномерного доступа к информационным технологиям в различных регионах страны;
* низкий уровень производства компьютерного оборудования, ПО, телекоммуникационного оборудования;
* низкий уровень развития электронной промышленности;
* нехватка квалификационных кадров в области ИТ.

Для того, чтобы информационные технологии развивались и приносили хороший эффект, они требуют вложений, таких как:

* финансирование прежде всего со стороны государства и инвестиционные вложения;
* разработка государственных и коммерческих программ по эффективному ИТ-технологий;
* высококвалифицированные ИТ-специалисты;
* система лояльности в отношении налогообложения производителей ПО;
* ужесточение законодательства в области охраны интеллектуальной собственности.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Беларуси. Поэтому решение вопроса об разработке эффективной политики информационной безопасности на современном предприятии обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации.

Разработку мер защиты информации целесообразно начинать с угроз, имеющих максимальное значение; далее - с меньшей угрозой, и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы. Такой подход гарантирует, что даже при малых ресурсах хватит ресурсов для предотвращения наиболее значимых угроз. Для каждой угрозы разрабатываются меры (способы и средства) по защите информации.

Политика информационной безопасности определяет, что мы хотим защитить и что ожидается от пользователей системы. Правила информационной безопасности описывают непосредственные обязанности пользователя, такие как защита конфиденциальной информации и создание нетривиальных паролей.

Политика ИБ направлена на обеспечение информационной безопасности ИС и связанны с ней ресурсов.

Цели политики информационной безопасности поликлиники:

* защита ИС от угроз, исходящих от противоправных действий злоумышленников;
* уменьшение рисков;
* снижение потенциального вреда от ошибочных действий персонала;
* уменьшение вреда от технических сбоев;
* передача и хранение информации.

Задачи политики информационной безопасности поликлиники:

* выделение и классификация особенностей ИС поликлиники;
* обеспечение необходимого уровня защиты информации ИС;
* выявление всех возможных угроз и их источников;
* разработка концепции ПИБ для поликлиники;
* разработка мероприятий по внедрению политики безопасности.

# **Объекты защиты**



Рисунок 2.1 – Структура поликлиники

В структуру поликлиники входят следующие службы:

* административно-управленческая часть;
* регистратура;
* лечебно-профилактические отделения;
* отделения восстановительного лечения;
* консультативно-диагностическое отделение;
* отделение медико-социальной помощи;
* дневной стационар;
* отделение неотложной медицинской помощи;
* профильные кабинеты;
* вспомогательные подразделения.

В состав административно-управленческой части входят: главный врач (заведующий), заместители главного врача, главная (старшая) медицинская сестра. Во главе поликлиники стоит главный врач, у него имеется три заместителя: по лечебной работе – начмед, по экспертным вопросам и по хозяйственным вопросам – завхоз.

Основными составляющими регистратуры являются:

* вызов врача на дом;
* справочная;
* кабинет учета и хранения листов нетрудоспособности.

В состав лечебно-профилактического отделения входят:

* хирургическое отделение;
* терапевтическое отделение;
* кабинет доврачебного приема;
* процедурный кабинет;
* прививочный кабинет;
* диагностические кабинеты;
* кабинет ЭВМ;

Отделение восстановительного лечения состоит из:

* кабинета физиотерапии;
* кабинета ЛФК;
* кабинета массажа;
* кабинета логопедии;
* кабинета иглорефлексотерапии.

В состав консультативно-диагностического отделения входят следующие кабинеты:

* кабинеты врачей-специалистов;
* кабинеты функциональной диагностики;
* кабинеты лучевой диагностики;
* кабинет ультразвуковой диагностики;
* кабинет рентгенологический;
* клинико-биохимическая лаборатория.

Отделение медико-социальной помощи состоит из кабинетов:

* терапевта;
* психолога;
* юриста;
* логопеда;
* социального работника;

В состав вспомогательных подразделений входят:

* кабинет учета и медицинской статистики;
* аптека;
* хозяйственная часть;
* хозрасчетные отделения и отделения дополнительных услуг.

К профильным кабинетам относят аллергологический, кардиологический, неврологический, травматолого-ортопедический, оториноларингологический, педиатрический, офтальмологический и другие кабинеты.

Также на территории поликлиники существует централизованная бухгалтерия, которая состоит из расчетной и материальной группы, отдел кадров, планово-экономический отдел, а также технический отдел.

Регистратура обеспечивает формирование и распределение потока пациентов, своевременную запись и регистрацию больных на прием к врачу, в том числе с применением информационных технологий. Непосредственное руководство работой регистратуры осуществляет старшая медицинская сестра поликлиники, главный врач амбулатории, назначаемые на должность и освобождаемые от должности руководителем медицинской организации. Основными задачами регистратуры являются:

* организация беспрепятственной и безотлагательной предварительной записи на прием к врачу, в том числе в автоматизированном режиме, в кабинет медицинской профилактики, кабинет доврачебной помощи (как при непосредственном обращении в поликлинику, так и по телефону);
* организация и осуществление регистрации вызовов врачей на дом по месту жительства (пребывания) больного;
* систематизированное хранение медицинской документации пациентов, обеспечение своевременного подбора и доставки документации в кабинеты врачей;
* направление граждан, в установленном порядке, на профилактические обследования и осмотры.

Дневной стационар – это своеобразный промежуточный вариант между амбулаторным режимом и стационарным лечением. Он организуется для осуществления лечебных и диагностических мероприятий при заболеваниях и состояниях, не требующих круглосуточного медицинского наблюдения.

Главный врач поликлиники – это в первую очередь абсолютная компетентность в вопросах клинической медицины. Он должен знать, уметь и использовать современные технологии управленческого процесса, обеспечить реализацию принятых решений, организовать работу коллектива по оказанию своевременной и качественной медицинской и лекарственной помощи населению, обеспечивать организацию лечебно-профилактической, административно-хозяйственной и лекарственной помощи населению, контролировать выполнение требований правил внутреннего трудового распорядка, техники безопасности, охраны труда, технической эксплуатации приборов, оборудования и механизмов.

В период отсутствия главного врача (командировка, отпуск, болезнь и др. причины) его обязанности возлагаются на заместителя главного врача, приобретающего соответствующие права и несущего ответственность за должное выполнение возложенных на него обязанностей.

Функции старшей медицинской сестры осуществляются по 4 направлениям: организационная работа, работа с персоналом, методическая работа и контроль за качеством оказываемой медпомощи. Однако, основное назначение старшей медсестры – это обеспечение медицинского учреждения медикаментами и расходными материалами, контроль за исправностью медицинского инструментария, контроль за питанием пациентов, рациональная организация и контроль за работой палатных медсестёр и младшего медицинского персонала, а также строгое соблюдение фармацевтического порядка.

Отдел неотложной медицинской помощи осуществляет медицинскую помощь гражданам при заболеваниях, несчастных случаях, травмах, отравлениях и других состояниях, требующих срочного медицинского вмешательства.

Диагностическое отделение – это отделение, где проводится целенаправленное исследование для оценки здоровья, состояния и функций органов и систем, физического и психического развития, профессиональной пригодности, с целью профилактики, диспансеризации, а также для определения природы заболевания.

В отделении восстановительного лечения осуществляется ударно-волновая терапия, для лечения болевых синдромов опорно-двигательного аппарата, а также программа реабилитации после травм и ортопедических операций, в том числе на коленном и тазобедренном суставах.

Также оказывается помощь определенного типа в профильных кабинетах и лечебно-профилактическом отделении.

Таким образом, предоставление медицинских услуг гражданам требует достаточно обширного количества медицинских работников и оборудования.

Основными объектами защиты системы информационной безопасности в поликлинике являются:

* информационные ресурсы, содержащие конфиденциальную информацию, коммерческую тайну, персональные данные пациентов и сотрудников, сведения ограниченного распространения;
* носители информации всех видов;
* информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена, системы и средства защиты информации, объекты и помещения.

Основные типы защищаемых активов поликлиники:

* + коммерческая тайна;
  + инсайдерская информация;
  + персональные данные.

Основными субъектами защиты системы информационной безопасности в поликлинике являются:

* + сотрудники поликлиники;
  + клиенты;
  + компьютерное аппаратное обеспечение;
  + партнеры учреждения.

# **Основные угрозы и их источники**

Угроза информационной безопасности – совокупность условий и факторов, создающих опасность нарушения информационной безопасности. Под угрозой, в общем случае, понимается потенциально возможное событие, процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

В зависимости от критериев, угрозы можно разделить на:

­­­­­­­­­– естественные и искусственные;

– внешние и внутренние;

– преднамеренные и непреднамеренные.

К внутренним угрозам относят:

– нарушение эксплуатации аппаратных средств;

– ошибки в базах данных, приводящие к модификации данных;

– системные ошибки.

К внешним:

– доступ к данным сотрудниками, не имеющих достаточных прав;

– человеческий фактор;

– НСД к данным сотрудников и клиентов поликлиники, приводящий к модификации информации.

К естественным:

– перебои в электроснабжении;

– различные климатические условия.

К искусственным:

– доступ к данным сотрудниками, не имеющих достаточных прав;

– человеческий фактор;

– заражение компьютерных систем вирусами и вредоносными программами;

– НСД к данным сотрудников и клиентов поликлиники, приводящий к модификации информации. ы

Среди угроз так же существуют преднамеренные и непреднамеренны.

Преднамеренные:

– НСД к данным поликлиники, с целью получения какой-либо выгоды;

– неправомерный доступ к носителям данных поликлиники.

Непреднамеренные:

– нарушение целостности данных сотрудниками, в виду случайных ошибок/невнимательности сотрудников;

– ошибки в работе с данными в виду отсутствия опыта у сотрудников поликлиники;

– ошибки в использовании программных средств и эксплуатации аппаратных средств.

Человеческий фактор является, наверное, самой главной угрозой информационной безопасности и зависит от человеческих отношений напрямую. Чаще всего, это ошибочные действия и/или нарушения, связанные с недобросовестностью, халатностью, безответственность, некомпетентностью. К ошибочным действиям, в частности, относятся:

* непредумышленное искажение или удаление информации (электронных документов);
* нарушение правил хранения ключевой, аутентифицирующей информации, а также любой другой информации ограниченного доступа;
* предоставление неавторизованным пользователям возможности обработки информации ограниченного доступа, доступа к средствам защиты информации, а также к техническим программным средства, способным повлиять на выполнение предъявляемых к средствам защиты информации требований; внедрение и использование неучтенных программ.

Любое лицо, имеющее физический или логический доступ к информационному ресурсу и компонентам соответствующих информационных технологий (программному обеспечению и данным, средствам вычислительной техники, коммуникационному оборудованию и каналам связи), может являться потенциальным злоумышленником. При это существует вариант сговора работника поликлиники с внешним злоумышленником, но не сговор двух и более сотрудников поликлиники.

# **Оценка угроз, рисков и уязвимостей**

Риск является неотъемлемым элементов экономической, политической и социальной жизни общества, который неизбежно сопровождает все направления и сферы деятельности любой организации. В общем виде риск – это вероятность возникновения определенного уровня отклонений от ожидаемого результата.

С развитием информационных технологий появляется все больше и больше угроз безопасности информации. Информация используется в бизнес-проектах для облегчения введения бизнеса. Таким образом, можно заметить, что увеличение влияния уровня безопасности информационных систем на успех в введении бизнеса и на возможность введения бизнеса в целом.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационных систем поликлиники. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Поэтому безопасность информационных систем - один из важнейших вопросов, который привлекает большое внимание со стороны аналитиков, инженеров и других специалистов в области информационной безопасности.

Риск характеризует опасность, которой может подвергаться система и использующая её организация. Риск зависит от показателей ценности ресурсов, вероятности реализации угроз для ресурсов и степени легкости, с которой уязвимости могут быть использованы при существующих или планируемых средствах обеспечения информационной безопасности.

Чтобы снизить уровень риска и минимизировать его негативные последствия, необходимо проводить измерение и оценку рисков.

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и её ресурсов. На основании оценивания рисков выбираются средства, обеспечивающие режим информационной безопасности. Систематическая оценка рисков проводится на основе качественных и количественных методов.

Ресурсы, считаются подверженными риску, если по отношению к ним существует какая-либо угроза.

При оценке рисков учитывается:

* ценность ресурсов,
* оценка экономических угроз,
* эффективность существующих средств защиты.

Основными рисками информационной безопасности являются:

* риск утечки конфиденциальной информации. Разглашение конфиденциальной информации приводит к прямым материальным убыткам, потере интеллектуальной собственности, снижению репутации организации и уровня доверия клиентов и партнеров. Кроме того, увеличивается риск финансовой ответственности поликлиники за нарушение правовых норм, регулирующих процессы обработки конфиденциальных данных;
* риск потери или недоступности важных данных. Угроза потери данных существует как при хранении, так и при работе с данными. При этом данные могут быть потеряны по причине сбоев энергоснабжения, оборудования, ошибок программного обеспечения, а также из-за ошибки пользователя или намеренного вредительства;
* риск использования неполной или искаженной информации;
* риск неполадок и сбоев в системе;
* риск несчастных случаев на производстве в связи с поломками оборудования;
* риск потери управления в связи с неполадками в электропитании
* риск распространения во внешней среде информации, угрожающей репутации организации.

Анализ рисков состоит в том, чтобы выявить существующие риски и предложить способ их оценки.

Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами:

* количественными (например, стоимостные);
* качественными (могут быть построены на использовании таких понятий, как, умеренный или чрезвычайно опасный);
* их комбинацией.

Таблица 4.1 – Условная численная шкала для оценки ущерба

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб поликлинике |
| 1 | Ущерб от атаки есть, но незначительны, основные финансовые операции и положение издательства на рынке не затронуты |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время поликлиника терпит убытки, но количество пациентов и статус изменяются минимально |
| 3 | Значительные потери в прибыли. От издательства уходит ощутимая часть клиентов. Теряется статус поликлиники |
| 4 | Потери очень значительны, поликлиника теряет статус (на срок до 2 лет). Для восстановления статус и положения в медицинской области требуются финансовые средства |
| 5 | Поликлиника прекращает существование |

В таблице 4.1 представлена шкала численной оценки рисков от НСД к информационным ресурсам поликлиники.

чтобы конкретизировать определение вероятности в течение которого предполагается защитить ресурс. Вероятность того, что угроза реализуется, определяется следующими факторами:

* привлекательность ресурса как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
* возможность использования ресурса для получения дохода;
* технические возможности угрозы, используемые при умышленном воздействии со стороны человека;
* вероятность того, что угроза реализуется;
* степень легкости, с которой уязвимость может быть использована.

Создадим шкалу вероятности того, что угроза будет реализована (таблица 4.2)

Таблица 4.2 – Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам.

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

Далее создаем таблицу оценки рисков (таблица 4.3). На этапе анализа таблицы риски задаются некоторым максимально допустимым уровнем (порогом), например, значением 0,5.

Таблица 4.3 — Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Атака | Ущерб | Вероятность | Риск |
| НСД к данным сотрудников поликлиники | 4 | 0,2 | 0,8 |
| Отказ и неисправность техники | 2 | 0,3 | 0,6 |
| Спам (переполнение почтового ящика) | 1 | 0,4 | 0,4 |
| Отключение электропитания на длительное время | 1 | 0,2 | 0,2 |
| DDOS | 2 | 0,3 | 0,6 |
| Доступ к данным сотрудниками, без достаточных прав | 1 | 0,4 | 0,4 |
| Потеря данных в результате несанкционированного доступа | 3 | 0,2 | 0,6 |
| Непреднамеренные ошибки сотрудников | 1 | 0,5 | 0,5 |
| Парольные атаки | 4 | 0,2 | 0,8 |
| Стихийные бедствия и аварии | 2 | 0,1 | 0,2 |
| Кражи и взломы | 3 | 0,1 | 0,3 |
| Заражение компьютерных систем вирусами и вредоносными программами | 2 | 0,4 | 0,8 |
| Проникновение посторонних на рабочие места | 3 | 0,1 | 0,3 |
| Сбои в базах данных | 3 | 0,2 | 0,6 |
| Итого |  |  | 7,1 |

Этап оценки рисков является чрезвычайно важным, так как он определяет дальнейшие действия и директивы поликлиники в области безопасности

# **Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов**

Целями защиты информации являются: предотвращение утечки, хищения, угрозы, утраты, искажения, подделки информации; предотвращение угроз безопасности личности, общества и государства; предотвращение несанкционированных действий по уничтожению, копированию и блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

В целях защиты информационных активов производится регулярное повышение осведомленности работников в области обеспечения защиты информации. Порядок повышения осведомленности работников описан во внутренних документах поликлиники.

Опираясь на риски, собранные в предыдущем пункте, можно описать меры защиты информации поликлиники.

Для защиты от отказов и неисправности технических средств предполагается наличие специалистов или отделов отвечающих за ремонт технических средств. Для отсутствия краж и взломов требуется наличие охраны, а также камер видеонаблюдения.

Для того, чтобы избежать отключения электропитания на длительное время необходимо наличие источников резервного электропитания.

Для защиты от атак типа man-in-the-middle требуется использование шифрованных данных.

Для отсутствия парольных атак необходимы одноразовые пароли либо криптографическая аутентификация.

Также можно предусмотреть другие меры защиты информации:

* меры технологического характера, имеющие целью повысить надежность процедуры передачи информации платежной системы и идентификации владельца карточки;
* обеспечение информационной безопасности при использовании ресурсов Internet;
* использование сети Internet сотрудниками издательства;
* использование электронной почты, как внутрикорпоративной, так и через Internet;
* обеспечение безопасности информации в автоматизированных системах;
* архивы электронной информации;
* радиоизлучения или электрические сигналы от внедренных специальных электронных устройств перехвата информации;
* акустическое излучение информативного речевого сигнала;
* просмотр информации с экранов дисплеев и других средств ее отображения визуально и с помощью оптических средств;
* размещение компьютерного и телекоммуникационного оборудования;
* регистрация пользователей и использование паролей на уровне операционных систем, прикладного программного обеспечения и компьютерной сети;
* управление доступом на уровне операционных систем, прикладного программного обеспечения и компьютерной сети;
* защита от вирусов и других вредоносных программ;
* системы мониторинга безопасности операционных систем, прикладного программного обеспечения и компьютерной сети;
* системы сканирования безопасности операционных систем, прикладного программного обеспечения и компьютерной сети;
* средства аудита безопасности операционных систем, прикладного программного обеспечения и компьютерной сети;
* анализаторы протоколов, ведущихся операционными системами, прикладным программным обеспечением и устройствами компьютерной сети;
* резервное копирование данных. Это решение, подразумевающее хранение важной информации не только на конкретном компьютере, но и на других устройствах: внешнем носителе или сервере. В последнее время особенно актуальной стала услуга удаленного хранения различной информации в «облаке» дата-центров. Именно такое копирование способно защитить компанию в случае чрезвычайной ситуации, например, при изъятии сервера органами власти. Создать резервную копию и восстановить данные можно в любое удобное для пользователя время, в любой географической точке.
* план аварийного восстановления данных. Крайняя мера защиты информации после потери данных. Такой план необходим каждой поликлиники для того, чтобы в максимально сжатые сроки устранить риск простоя и обеспечить непрерывность бизнес-процессов. Если компания по каким-то причинам не может получить доступ к своим информационным ресурсам, наличие такого плана поможет сократить время на восстановление информационной системы и подготовки ее к работе. В нем обязательно должна быть предусмотрена возможность введения аварийного режима работы на период сбоя, а также все действия, которые должны быть предприняты после восстановления данных. Сам процесс восстановления следует максимально отработать с учетом всех изменений системы.
* анти-DDoS. Грамотная защита от DDoS-атак собственными силами невозможна. Многие разработчики программного обеспечения предлагают услугу анти-DDoS, которая способна защитить от подобных нападений. Как только в системе обнаруживается трафик необычного типа или качества, активируется система защиты, выявляющая и блокирующая вредный трафик. При этом бизнес-трафик поступает беспрепятственно. Система способна срабатывать неограниченное количество раз, до тех пор, пока угроза не будет полностью устранена.
* шифрование данных при передаче информации в электронном формате (end-to-end protection).

Чтобы обеспечить конфиденциальность информации при ее передаче в электронном формате применяются различные виды шифрования. Шифрование дает возможность подтвердить подлинность передаваемой информации, защитить ее при хранении на открытых носителях, защитить программное обеспечение и другие информационные ресурсы поликлиники от несанкционированного копирования и использования.

* антивирусные программы – программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом.
* организацию охраны помещений, в которых содержатся носители конфиденциальной информации;
* установление режима работы в помещениях, в которых содержатся носители конфиденциальной информации;
* установление пропускного режима в помещения, содержащие носители конфиденциальной информации;
* закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;
* установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);
* организацию ремонта технических средств обработки конфиденциальной информации;
* организацию контроля за установленным порядком.

Технические мероприятия по обеспечению информационной безопасности заключаются в обслуживании, поддержке и управлении составом технических средств поликлиники, обеспечивающих обработку информации ограниченного доступа в поликлинике в защищенном режиме. Технологические мероприятия по обеспечению безопасности информации направлены на реализацию заданных функций и алгоритмов работы поликлиники, технологий обработки информации ограниченного доступа и защиту программ и данных от преднамеренных и непреднамеренных нарушений.

Также необходимо оснастить каждое отделение, в частности кабинет, фильтрами бесперебойного питания, а также собственным генератором; ужесточить пропускной режим, ввести проход по талонам либо кодам персональных карточек; резервная копия БД, хранящаяся не только на одном персональном компьютере, а также наличие качественных дверей и окон и сигнализаций.

Для обеспечения актуальности модели угроз должен осуществляться ее плановый (регулярный) и внеплановый пересмотр. Плановый пересмотр проводится с периодичностью не реже чем один раз в два года.

# **Вывод**

В ходе лабораторной работы были проанализированы риски, связанные с информационной безопасностью поликлиники. Были предусмотрены явления, которые могут оказать влияние на целостность системы и вывести ее из строя. Разработанная политика безопасности не способна обеспечить полную защиту всей информации, но она необходима для обеспечения некоторых гарантий.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Со временем могут возникать новые каналы утечки или способы взлома, которые ранее не были рассмотрены службой безопасности. Подобные происшествия нужно мониторить и устранять в максимально короткие сроки.

Для ознакомления сотрудников с правилами разграничения доступа и тонкостями организации безопасности следует регулярно проводить служебные тренинги или выдавать служебные инструкции по использованию техники и ведению документации.

Эффективное выполнение политики безопасности подразумевает создание системы защиты конфиденциальных данных предприятия с минимальными затратами и максимальным охватом всех возможных каналов утечки данных

Прежде чем внедрять какие-либо решения по защите информации, необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. Политику безопасности желательно оформить в виде отдельного документа и утвердить руководством предприятия. Система информационной безопасности окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот.