Учреждение образования

«Белорусский государственный технологический университет»

**Отчет к лабораторной работе №1**

по дисциплине «Защита информации и надежность информационных систем»

Выполнил:

Студент 3 курса 5 группы ФИТ

Димитриади Антон Владимирович

**Разработка и внедрение политики безопасности организации или учреждения**

**Цель:** приобретение практических навыков разработки и внедрения эффективной политики информационной безопасности организации или учреждения.

**Задачи:**

1. Научиться выделять и классифицировать особенности информационной или информационно-вычислительной системы (ИВС) конкретной организации или учреждения как объекта защиты.

2. Овладеть навыками принятия обоснованных решений по организационному и правовому регулированию проблем, относящихся к состоянию безопасности ИВС, обеспечению необходимого уровня защиты информации в ИВС.

3. Овладеть основными приемами анализа угроз информационной безопасности ИВС.

4. Научиться выявлять все возможные угрозы и их источники информационной безопасности в организации или учреждении, анализировать и оценивать собранные данные.

5. Разработать концепцию, основные элементы политики безопасности для организации или учреждения по указанному преподавателем варианту задания.

6. Разработать мероприятия по внедрению предложенной Вами политики безопасности.

7. Результаты выполнения лабораторной работы оформить в виде описания разработанной политики безопасности, а также плана мероприятий по ее реализации.

**Введение**

Cегодня невозможно представить практически ни одну сферу деятельности без средств вычислительной техники и телекоммуникаций. Информационные технологии предлагают все новые и новые сервисы. Через Интернет становятся доступными электронные платежные системы, персональные финансовые порталы, электронные биржи и т. д. Внедряя новые услуги, компании укрепляют свое положение на рынке. С другой стороны, вопросы информационной безопасности всегда, как минимум, на шаг отстают от нововведений. Достаточно посмотреть, сколько версий должно миновать, пока тот или иной программный продукт не приобретет репутацию надежного. Эти две очевидные тенденции приводят к необходимости здорового консерватизма в построении информационных систем корпоративного уровня. Нужен взвешенный подход, учитывающий риски и стоимость отдачи от вложенных средств. Информационные технологии все шире применяются в качестве инструментоведения бизнеса. И понятие риска является краеугольным как для бизнеса, так и для системы организации информационной безопасности. Но при этом следует понимать, что стандарты и передовые практики обычно не рассматривают конкретные программы и детальные методики, а концентрируются на основных принципах и примерах. С точки зрения рисков следует иметь в виду два аспекта:

- Во-первых, любую систему безопасности можно взломать, имея достаточно ресурсов и времени. Поэтому риски могут быть идентифицированы и уменьшены, но никогда не сведены полностью на нет.

- Во-вторых, все организации разные, поэтому процесс смягчения рисков для каждой имеет свои уникальные черты.

**Цели разработки ПИБ:**

* Защита конфиденциальности медицинских данных пациентов и персональных данных сотрудников больницы от несанкционированного доступа, использования или раскрытия.
* Обеспечение доступности, целостности и конфиденциальности информации в системах здравоохранения больницы, чтобы гарантировать надежность и точность медицинской информации.
* Повышение осведомленности сотрудников больницы о мероприятиях по обеспечению безопасности информации и их роли в этом процессе.
* Обеспечение надежной и безопасной работы с информационными системами и технологиями больницы.

**Задачи разработки ПИБ:**

* Разработка и внедрение политики и процедур информационной безопасности для всех сотрудников больницы.
* Определение уровней доступа к медицинской информации, управление учетными записями и аудит действий пользователей системы.
* Разработка и регулярное проведение аудитов информационной безопасности, оценка рисков и управление их минимизацией.
* Обеспечение защиты информационных систем от вредоносного программного обеспечения и других угроз безопасности.
* Обучение сотрудников больницы основам безопасности информации и проведение регулярных тренингов и обучений.
* Управление инцидентами, связанными с нарушением безопасности информации, и разработка планов действий для предотвращения и реагирования на такие инциденты.
* Разработка процедур бэкапа данных и восстановления систем в случае чрезвычайных ситуаций.
* Проведение регулярных аудитов соответствия политики информационной безопасности требованиям и нормативным актам.

**Описание структуры**

Больница – это лечебно-профилактическое учреждение здравоохранения, в котором оказывается специализированная медицинская помощь в условиях стационара.

Основные задачи больниц:

* оказание медицинской помощи при невозможности лечения или проведения сложных диагностических исследований в амбулаторно-поликлинических условиях;
* оказание медицинской помощи в случае, если выздоровление или улучшение состояния пациента в стационаре может быть достигнуто быстрее, чем при амбулаторном лечении;
* оказание медицинской помощи пациентам, пребывание которых в домашних условиях представляет угрозу для окружающих (при инфекционных, венерических заболеваниях, некоторых видах психических расстройств).

В зависимости от территории обслуживания все больницы делятся на:

* городские – комплексная лечебно-профилактическая стационарная помощь оказывается населению всего города или его части;
* областные – специализированная стационарная и амбулаторно-консультативная медицинская помощь оказывается населению определенной области;
* центральные районные – специализированная медицинская помощь и организационно-методическое руководство здравоохранением оказывается населению района;
* участковые – специализированная медицинская помощь оказывается сельскому населению по основным специальностям (терапия, педиатрия, хирургия, акушерство, инфекционные заболевания);
* больницы сестринского ухода – медико-социальная помощь оказывается гражданам, которые страдают хроническими заболеваниями и нуждаются в постоянном круглосуточном медицинском наблюдении и уходе, но которым не требуется оказание медицинской помощи в стационарных условиях.

От того, в какой мере и насколько качественно решаются данные задачи, зависит объем работы других медицинских организаций, а также многие показатели, характеризующие деятельность системы здравоохранения в целом.

Руководство больницей осуществляет главный врач, который имеет заместителей. В многопрофильных больницах могут вводится должности заместителя главного врача по отдельным направлениям работы (по медицинской части, по хирургии, по организационно-методической работе, по экспертизе трудоспособности, по хозяйственной работе, по внебюджетной деятельности, по гражданской обороне). При наличии в структуре поликлиники - заместителя главного врача по поликлинической работе.

Регистратура является основным структурным подразделением по организации приема больных. В функции регистратуры входит:

- регистрация первичных пациентов;

- организация предварительной и неотложной записи больных на прием к врачу как при непосредственном обращении в больницу, так и по телефону;

- обеспечение регулирования интенсивности потока пациентов с целью создания равномерной загрузки врачей и распределения пациентов по видам оказываемой помощи.

Структура больницы представлена на рисунке ниже:

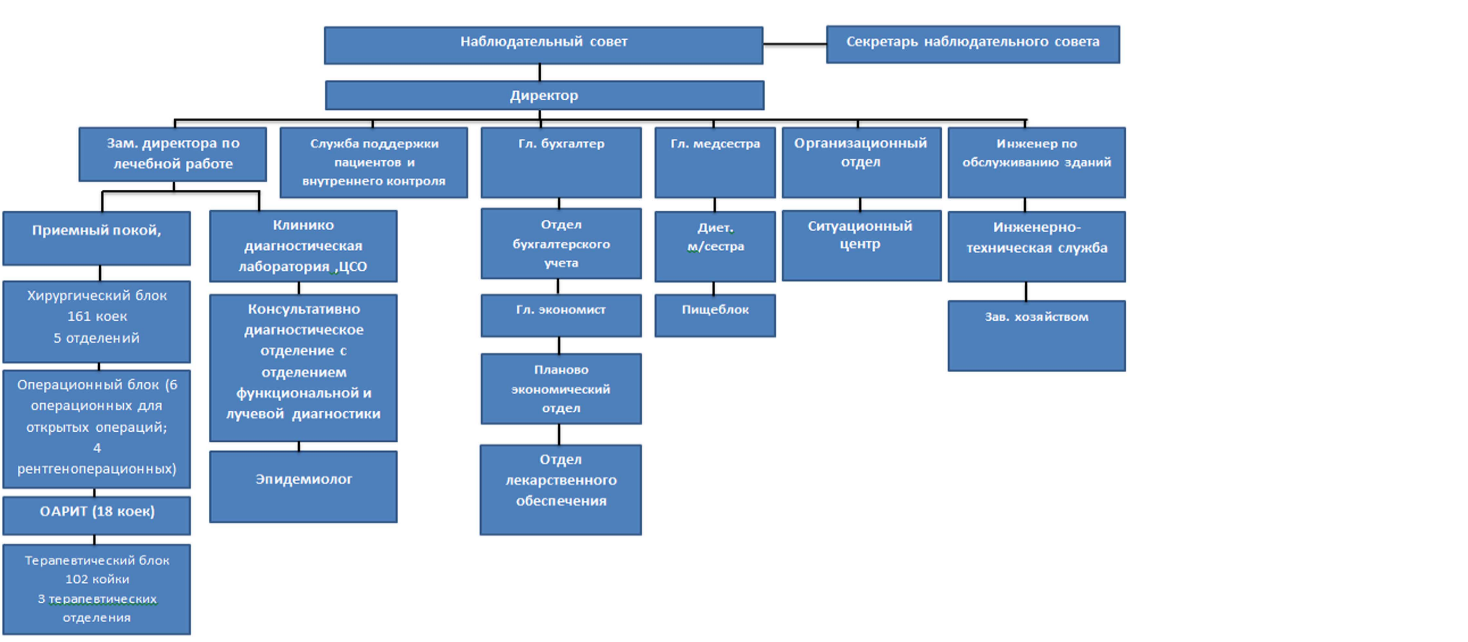


Рисунок 1 — Структура больницы

**К объектам защиты медицинской информационной системы относят:**

* сведения в базе данных;
* резервные и архивные копии сервера;
* целевые данные администратора и начальника;
* средства обеспечения функционирования медицинской информационной системы;
* обработка информации в медучреждении – сбор, хранение, передача;
* производительность файлового сервера.

**К субъектам защиты медицинской информационной системы относятся:**

* Медицинские работники, включая врачей, медсестер, лаборантов и других специалистов, которые имеют доступ к медицинской информации.
* Административный персонал, который управляет медицинской информационной системой и контролирует доступ к данным.
* Пациенты, чьи медицинские данные хранятся в системе, и которые имеют право на доступ к своей личной информации.
* Посторонние пользователи, которые могут попытаться получить несанкционированный доступ к медицинской информации, включая злоумышленников, хакеров и других киберугроз.
* Регулирующие органы, которые могут проверять систему на соответствие нормам и требованиям законодательства в области медицинской информационной безопасности.
* Консультанты и подрядчики, которые могут иметь доступ к системе в рамках выполнения своих профессиональных обязанностей.
* Компьютер.

**Источники угроз и их классификация**

Классификация угроз в основном делится на два вида: *естественные* и *искусственные*.

*Естественные* угрозы - это угрозы, которые возникают в результате природных катастроф, таких как землетрясения, цунами, ураганы, пожары и т.д. Естественных угрозы:

* Потеря электропитания: природные катастрофы могут привести к потере электропитания, что может привести к неработоспособности системы хранения и обработки медицинской информации.
* Потеря связи: природные катастрофы могут привести к потере связи, что может привести к невозможности получения доступа к медицинской информации.
* Уничтожение физических устройств: природные катастрофы могут привести к уничтожению физических устройств, таких как компьютеры, серверы, роутеры, которые хранят и обрабатывают медицинскую информацию.
* Потеря квалифицированных специалистов: природные катастрофы могут привести к потере квалифицированных специалистов, что может привести к нарушению информационной безопасности больницы, так как не будет достаточного числа сотрудников для обеспечения безопасности информации.
* Ухудшение условий хранения медицинской информации: природные катастрофы могут привести к ухудшению условий хранения медицинской информации, например, при пожаре или наводнении, что может привести к её повреждению и утрате.
* Нарушения безопасности у поставщиков услуг: когда поставщики услуг, работающие с больницей, не соблюдают правила информационной безопасности, что может привести к утечке конфиденциальной информации.

*Искусственные* угрозы - это угрозы, которые создаются или порождаются человеком, а не природой. Искусственных угрозы:

* Кибератаки: злоумышленники могут использовать различные методы, такие как фишинг, вирусы и взломы, чтобы получить несанкционированный доступ к медицинской информации и использовать её для мошенничества или кражи личных данных.
* Внутренние угрозы: сотрудники больницы могут неумышленно или преднамеренно нарушать политику безопасности, например, раскрывать конфиденциальную информацию или создавать уязвимости в системе.
* Угрозы физической безопасности: кража или утеря медицинских устройств, на которых хранится конфиденциальная информация, или несанкционированный доступ к ним.
* Социальная инженерия: злоумышленники могут использовать обман и манипуляцию, чтобы убедить сотрудников или пациентов раскрыть свою конфиденциальную информацию или предоставить доступ к системе.
* Внешние угрозы: конкуренты, хакерские группировки или другие злоумышленники могут использовать различные методы, чтобы получить несанкционированный доступ к медицинской информации, взломать систему или украсть данные.

Источники угроз по отношению к самой информационной системе могут быть как *внешними*, так и *внутренними*.

К *внешним* угрозам относятся:

* Хакерские атаки: когда злоумышленники пытаются проникнуть в систему больницы, чтобы получить доступ к медицинской информации или нанести ущерб.
* Вирусы и другие вредоносные программы: когда злоумышленники используют вредоносные программы, чтобы получить доступ к медицинской информации или нанести ущерб системе больницы.
* Фишинг: когда злоумышленники пытаются получить доступ к медицинской информации, используя поддельные электронные письма, веб-сайты или социальные сети.
* Атаки отказа в обслуживании (DDoS): когда злоумышленники пытаются перегрузить сеть больницы, чтобы она стала недоступной для других пользователей.
* Физические угрозы: когда злоумышленники пытаются получить физический доступ к серверам и компьютерам больницы, чтобы получить доступ к медицинской информации или нанести ущерб системе.

К *внутренним* угрозам относятся:

* Несанкционированный доступ к медицинской информации: сотрудники больницы могут получать доступ к медицинской информации, которая не относится к их работе, что может привести к утечке конфиденциальных данных.
* Нарушение политики безопасности: сотрудники больницы могут не соблюдать правила информационной безопасности, такие как использование слабых паролей или оставление компьютеров включенными без присмотра.
* Утеря или кража устройств: сотрудники больницы могут утерять или украсть устройства, содержащие конфиденциальную медицинскую информацию, такие как ноутбуки, смартфоны и USB-накопители.
* Несанкционированный доступ к помещениям: сотрудники больницы могут получать несанкционированный доступ к помещениям, в которых находятся компьютеры, серверы и другие устройства, содержащие конфиденциальную медицинскую информацию.
* Физический вред: сотрудники больницы могут наносить физический вред компьютерам, серверам и другим устройствам, содержащим конфиденциальную медицинскую информацию.
* Социальная инженерия: сотрудники больницы могут стать жертвами социальной инженерии, когда злоумышленники используют манипуляции и обман, чтобы получить доступ к конфиденциальной медицинской информации.

Так же существует разделение угроз на *преднамеренные* и *непреднамеренные*:

К *преднамеренным* угрозам относятся:

* Кибератаки: злоумышленники могут использовать различные методы, такие как фишинг, вирусы и взломы, чтобы получить несанкционированный доступ к медицинской информации и использовать её для мошенничества или кражи личных данных.
* Сотрудники больницы могут преднамеренно нарушать политику безопасности, например, раскрывать конфиденциальную информацию или создавать уязвимости в системе.
* Угрозы физической безопасности: кража или утеря медицинских устройств, на которых хранится конфиденциальная информация, или несанкционированный доступ к ним.
* Социальная инженерия: злоумышленники могут использовать обман и манипуляцию, чтобы убедить сотрудников или пациентов раскрыть свою конфиденциальную информацию или предоставить доступ к системе.
* Несанкционированный доступ к помещениям: сотрудники больницы могут получать несанкционированный доступ к помещениям, в которых находятся компьютеры, серверы и другие устройства, содержащие конфиденциальную медицинскую информацию.
* Физический вред: сотрудники больницы могут наносить физический вред компьютерам, серверам и другим устройствам, содержащим конфиденциальную медицинскую информацию.

К *непреднамеренным* угрозам относятся:

* Потеря электропитания: природные катастрофы могут привести к потере электропитания, что может привести к неработоспособности системы хранения и обработки медицинской информации.
* Потеря связи: природные катастрофы могут привести к потере связи, что может привести к невозможности получения доступа к медицинской информации.
* Уничтожение физических устройств: природные катастрофы могут привести к уничтожению физических устройств, таких как компьютеры, серверы, роутеры, которые хранят и обрабатывают медицинскую информацию.
* Потеря квалифицированных специалистов: природные катастрофы могут привести к потере квалифицированных специалистов, что может привести к нарушению информационной безопасности больницы, так как не будет достаточного числа сотрудников для обеспечения безопасности информации.
* Сотрудники больницы могут неумышленно нарушать политику безопасности, например, раскрывать конфиденциальную информацию или создавать уязвимости в системе.

**Оценка рисков**

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. 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.

**При оценивании рисков учитывается:**

* ценность ресурсов;
* оценка значимости угроз;
* эффективность существующих и планируемых средств защиты.

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

В самом широком смысле мера риска может рассматриваться в дальнейшем как описание видов неблагоприятных действий, воздействию которых может подвергнуться система или организация, и вероятностей того, что эти действия могут произойти. Результат этого процесса должен указать поликлинике степень риска, связанного с определенными ценностями. Этот результат важен, потому что он является основой для дальнейшего выбора средств защиты и решений по минимизации риска.

Таблица 1 — Условная численная шкала для оценки ущерба поликлиники

|  |  |
| --- | --- |
| **Величина ущерба** | **Описание** |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб поликлинике |
| 1 | Ущерб от атаки  есть, но он незначителен, основные финансовые операции не затронуты |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время поликлиника терпит убытки, но его положение на рынке и количество пациентов изменяются минимально |
| 3 | Значительные потери на рынке |
| 4 | Потери очень значительные, поликлиника теряет свое положение на рынке |
| 5 | Поликлиника прекращает свое существование |

**Хищение медицинских данных чревато следующими последствиями:**

* медицинские карты используются на черном рынке для получения медицинской помощи незастрахованными лицами;
* в карту могут быть внесены сведения вора, в результате пациент рискует получить помощь, основанную на чужой истории болезни, группе крови, непереносимости и аллергической реакции;
* мошенники могут исчерпать страховой лимит, и законный владелец лишится возможности получать медицинскую помощь в самое неподходящее время. Большинство страховых планов имеют ограничения на отдельные виды услуг. Например, страховая компания откажется оплачивать два оперативных вмешательства по удалению аппендицита;
* получив доступ к данным пациента, мошенники могут злоупотреблять рецептами на лекарства, лишив этой возможности владельца карты. Рецепты, как правило, лимитированные;
* если с устранением массовых кибератак на банковские карты проблемы не возникают, то защита от фишинговых атак потребует больших усилий.
* кража электронной медицинской карты может и вовсе остаться незамеченной. И если этот факт обнаруживается, то, как правило, в ситуациях, когда последствия угрожают жизни.

Таблица 2 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| **Описание атаки** | **Ущерб** | **Вероятность** | **Риск** |
| Спам | 1 | 0,4 | 0,4 |
| Копирование жесткого диска | 3 | 0,1 | 0,3 |
| Террористическая атака извне | 5 | 0 | 0 |
| Утечка персональных данных сотрудников или пациентов | 4 | 0,1 | 0,4 |
| Непреднамеренное искажение информации | 4 | 0,2 | 0,8 |
| Неавторизированный доступ | 1 | 0,5 | 0,5 |
| Землетрясения, наводнения, ураганы | 5 | 0 | 0 |
| Саботаж, забастовка | 2 | 0,1 | 0,5 |
| Отключение электричества | 2 | 0,2 | 0,4 |
| Вирусы | 2 | 0,3 | 0,6 |
| DDos атаки | 2 | 0,3 | 0,6 |
| Физические угрозы | 3 | 0 | 0 |
| Фишинг | 2 | 0,3 | 0,6 |
| Итого |  |  | 5,1 |

**Разработка мер защиты**

Есть и другие способы обеспечения безопасности, которые не относятся к медицинской информационной системе напрямую. Такие меры предполагают выполнение персоналом некоторых регламентов по работе с системой:

* организация охраны помещения, работы с документацией, сотрудниками. Использование технических средств и информационно-аналитической деятельности с целью выявления угроз – внутренних и внешних;
* исключение проникновения на территорию и в здание злоумышленников;
* организация работы с сотрудниками в части доступа к информации;
* обеспечение правильной работы с документами и документированными сведениями;
* задействование технических средств по сбору, накоплению, обработке и хранению конфиденциальных данных;
* организация работы по анализу угроз конфиденциальных сведений – внутренних и внешних;
* организация работы по выполнению контроля над работой сотрудников с информацией.

Построение системы защиты может выполняться в несколько этапов:

* собираются сведения о существующих информационных системах персональных сведений;
* моделируются угрозы безопасности;
* разрабатываются технические задания;
* проектируется система защиты информации;
* разрабатывается организационно-распорядительная документация, которая регламентирует процессы обработки и защиты сведений;
* поставляются, устанавливаются и настраиваются средства защиты информации;
* проводится аттестация информационных систем сведений, согласно требованиям безопасности.

Также внедряются и специализированные средства контроля доступа в помещение. Это могут быть:

* исполнительные устройства, включая кабины, турникеты, шлагбаумы;
* кардридеры, считывающие информацию;
* панели для введения кода с помощью клавиатуры;
* концентраторы и контроллеры;
* средства идентификации, включая брелоки, карты и биометрию;
* индивидуальное программное обеспечение.

С целью защиты данных пациента применяются несколько программных компонентов и механизмов. Для предотвращения несанкционированного доступа развертываются средства авторизации, внедряются системы обнаружения и предотвращения вторжений, а также утечек информации. Может устанавливаться антивирусное программное обеспечение. Существует успешная практика использования файерволов.

К криптографическим средствам защиты относят алгоритмы шифрования данных и внедрение электронной цифровой подписи. Системы аутентификации предполагают внедрение защиты с паролем, подпись сертификатами и открытие доступа по биометрическим данным.

Инструментальные средства анализа предполагают внедрение программного обеспечения для проведения мониторинга. К техническим относят комплексное внедрение технических средств защиты. Система бесперебойного питания предполагает установку, обслуживание источников бесперебойного питания, установку генераторов напряжения и резервирование нагрузки.

С целью предотвращения взлома и краж используются специальные средства, включая электронные ключи и смарт-карты. Эти технологии позволяют повысить уровень защиты информационной системы на этапе аутентификации.

**Вывод:** в ходе этой работы были проанализированы риски, связанные с информационной безопасностью больницы. 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 компании, 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.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. 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.