Практическое занятие №3

РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕС-КОМПАНИИ(БОЛЬНИЦА)

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Введение**

В современном мире медицинские учреждения сталкиваются с множеством угроз информационной безопасности, что требует комплексного и системного подхода к обеспечению защиты данных. Особенно важно учитывать, что медицинская информация является одной из наиболее конфиденциальных категорий данных, поскольку она включает в себя персональные сведения о пациентах, историю их лечения, медицинские заключения и иные сведения, которые не подлежат разглашению.

Любая утечка данных может привести к серьезным последствиям, включая нарушение врачебной тайны, потерю доверия пациентов и даже юридическую ответственность медицинского учреждения. В связи с этим разработка и внедрение политики информационной безопасности является необходимым шагом для предотвращения угроз, а также для эффективного реагирования на возможные инциденты.

Цель данной работы – разработка политики информационной безопасности для больницы, включающей основные угрозы, оценку рисков и меры защиты. В рамках данной политики рассматриваются механизмы обеспечения безопасности данных, такие как управление доступом, контроль сетевого трафика, резервное копирование, использование антивирусных средств и проведение обучающих мероприятий для персонала.

Данный документ представляет собой структурированный анализ всех аспектов информационной безопасности в медицинском учреждении и дает рекомендации по внедрению эффективных мер защиты. Политика информационной безопасности должна быть ориентирована на долгосрочную перспективу и учитывать возможные изменения в законодательстве, развитие технологий и появление новых угроз. Только системный подход позволит обеспечить надёжную защиту данных и создать безопасную цифровую среду в медицинском учреждении.

**2. Описание структуры больницы**

Современные медицинские учреждения представляют собой сложные организационные структуры, в которых осуществляется постоянный обмен данными между различными подразделениями. Больница включает в себя следующие подразделения:

* **Приёмное отделение** – занимается первичным осмотром и регистрацией пациентов, оформлением медицинской документации и направлением пациентов в соответствующие отделения.
* **Терапевтическое отделение** – обеспечивает амбулаторное лечение пациентов, диагностику заболеваний, ведение истории болезни и медицинских карт.
* **Хирургическое отделение** – проводит хирургические вмешательства и послеоперационный уход, требующий особой точности в обработке и хранении данных пациентов.
* **Реанимация** – специализированное отделение интенсивной терапии, где ведётся круглосуточный мониторинг пациентов, использующий медицинские приборы с интегрированными цифровыми системами.
* **Лаборатория** – выполняет диагностику заболеваний на основе лабораторных исследований, результаты которых должны храниться в защищённой базе данных.
* **Аптека** – отвечает за хранение и выдачу лекарственных препаратов, ведение электронных записей о движении медикаментов и интеграцию с другими системами больницы.
* **Администрация** – управляет финансовыми, кадровыми и юридическими вопросами учреждения, осуществляет бухгалтерский учет и формирует отчёты.
* **IT-отдел** – обеспечивает техническую поддержку всех информационных систем больницы, внедряет новые технологии защиты данных и контролирует сетевую безопасность.

Эффективное взаимодействие этих подразделений возможно только при надёжной системе информационной безопасности, минимизирующей риски несанкционированного доступа, утечек и сбоев в работе системы.

**3. Оценка рисков**

Классификация угроз информационной безопасности в больнице включает широкий спектр потенциальных рисков, с которыми может столкнуться медицинское учреждение:

* 1. **Несанкционированный доступ**
  + Проникновение злоумышленников в сеть больницы с целью кражи данных.
  + Использование слабых паролей сотрудниками.
  + Нарушение регламентов хранения информации.
  + Перехват сетевого трафика при недостаточной защите соединений.
  + Доступ к системам через уязвимости в устаревшем ПО.
  1. **Программные угрозы**
  + Вирусные атаки и вредоносные программы.
  + Использование устаревшего и уязвимого программного обеспечения.
  + Отсутствие регулярных обновлений и патчей безопасности.
  + Эксплуатация уязвимостей в операционных системах и сервисах.
  + Атаки типа «отказ в обслуживании» (DDoS) на критически важные сервисы больницы.
  1. **Аппаратные угрозы**
  + Выход из строя серверного оборудования.
  + Кража физических носителей информации.
  + Поломка рабочих станций и медицинского оборудования.
  + Неконтролируемый доступ к аппаратным средствам хранения данных.
  + Недостаточная резервная мощность серверов при пиковых нагрузках.
  1. **Человеческий фактор**
  + Ошибки сотрудников при работе с медицинской информацией.
  + Несоблюдение правил конфиденциальности.
  + Незнание основ информационной безопасности.
  + Использование личных устройств для работы с конфиденциальными данными.
  + Непреднамеренное удаление или изменение критически важных данных.
  1. **Социальная инженерия**
  + Фишинговые атаки.
  + Манипуляции, направленные на получение паролей.
  + Введение персонала в заблуждение для передачи критически важных данных.
  + Ложные звонки или письма от лиц, выдающих себя за руководство.
  + Использование соцсетей для сбора информации о персонале и организации атак.
  1. **Физическая безопасность**
  + Несанкционированный доступ к серверным комнатам.
  + Кража или подмена носителей информации.
  + Разрушение данных вследствие пожара, затопления или других чрезвычайных ситуаций.
  + Недостаточная защита от электромагнитных помех и внешних воздействий.
  1. **Внутренние угрозы**
  + Намеренные действия сотрудников, направленные на повреждение или утечку данных.
  + Конфликты внутри коллектива, приводящие к нарушению информационной безопасности.
  + Неконтролируемое копирование и распространение конфиденциальной информации.
  + Неавторизованное подключение сторонних устройств к внутренней сети больницы.
  1. **Правовые и регуляторные угрозы**
  + Нарушение требований законодательства о защите персональных данных.
  + Несоответствие внутренней политики безопасности требованиям государственных регуляторов.
  + Ненадлежащее ведение документации и журналов безопасности.
  + Недостаточный уровень подготовки сотрудников в области соблюдения правовых норм.

**4. Разработка мер защиты**

**4.1. Несанкционированный доступ**

* Внедрение многофакторной аутентификации (MFA) для всех сотрудников.
* Регулярное обновление паролей и использование сложных комбинаций.
* Шифрование сетевого трафика с использованием VPN и TLS.

**4.2. Программные угрозы**

* Использование актуального антивирусного ПО и систем обнаружения вторжений (IDS/IPS).
* Регулярное обновление операционных систем и установленного ПО.
* Разделение сетевого доступа для критически важных сервисов.

**4.3. Аппаратные угрозы**

* Создание резервных копий данных и настройка их автоматического обновления.
* Ограничение физического доступа к серверам и рабочим станциям (карточная система, видеонаблюдение).
* Использование ИБП (источников бесперебойного питания) для защиты от сбоев электропитания.

**4.4. Человеческий фактор**

* Проведение регулярного обучения персонала по вопросам информационной безопасности.
* Ограничение доступа сотрудников к данным на основе их должностных обязанностей (принцип минимально необходимого доступа).
* Разработка четких инструкций по работе с конфиденциальной информацией.

**4.5. Социальная инженерия**

* Фильтрация электронной почты для выявления фишинговых сообщений.
* Организация тренингов для сотрудников по выявлению попыток манипуляций.
* Введение политики запрета на передачу конфиденциальных данных по телефону или электронной почте без подтверждения личности.

**4.6. Физическая безопасность**

* Использование замков, биометрической аутентификации и систем видеонаблюдения в серверных помещениях.
* Хранение резервных носителей информации в защищенных сейфах.
* Разработка плана действий на случай пожара, наводнения и других чрезвычайных ситуаций.

**4.7. Внутренние угрозы**

* Мониторинг действий сотрудников в критически важных системах.
* Ограничение копирования и передачи конфиденциальных данных (DLP-системы).
* Запрет на использование личных устройств в корпоративной сети без разрешения.

**4.8. Правовые и регуляторные угрозы**

* Регулярные внутренние аудиты на соответствие законодательным требованиям.
* Разработка и внедрение политики информационной безопасности в соответствии с нормативными актами.
* Проведение обязательного обучения сотрудников по соблюдению норм защиты персональных данных.

**5. Выводы**

Таким образом, информационная безопасность в медицинском учреждении – это не просто отдельный аспект управления, а фундаментальная составляющая эффективного функционирования больницы. Современные угрозы, включая кибератаки, утечку данных и человеческий фактор, требуют тщательного подхода к защите информации, что достигается за счет комплексной политики безопасности, внедрения современных технологий защиты и регулярного обучения персонала.

В ходе исследования были определены основные угрозы, которым подвержена больница, и разработаны меры их предотвращения. Несанкционированный доступ, вредоносные программы, аппаратные сбои и социальная инженерия представляют серьезную угрозу не только для данных пациентов, но и для всей системы здравоохранения. В связи с этим важную роль играет не только внедрение защитных инструментов, но и разработка внутренних регламентов, направленных на минимизацию рисков.

Реализация предложенных мер, таких как многофакторная аутентификация, мониторинг сетевого трафика, резервное копирование, строгая политика управления доступом, применение антивирусных решений и повышение осведомленности персонала, позволит снизить вероятность инцидентов и создать безопасную среду для работы с медицинскими данными.

Кроме того, информационная безопасность не является статичной системой – она должна регулярно пересматриваться и адаптироваться к изменяющимся условиям, новым видам угроз и технологическим достижениям. Это требует постоянного взаимодействия между IT-специалистами, администрацией и медицинским персоналом.

Таким образом, разработка и внедрение политики информационной безопасности является ключевым фактором успешного функционирования медицинского учреждения. Обеспечение надежной защиты данных способствует не только выполнению нормативных требований, но и укреплению доверия пациентов, повышению эффективности работы больницы и улучшению качества оказываемых медицинских услуг. Долговременная стратегия защиты информации является важным условием для стабильного функционирования больницы в условиях цифровой трансформации медицины.

Также необходимо учитывать, что безопасность данных – это процесс, требующий постоянного совершенствования. Современные технологии быстро развиваются, появляются новые типы атак, поэтому больница должна быть готова оперативно реагировать на возникающие угрозы. Внедрение политики информационной безопасности способствует снижению рисков, повышению уровня защищённости данных и созданию эффективной инфраструктуры для хранения и обработки медицинской информации.

В конечном итоге надёжная защита данных – это не просто формальная необходимость, а залог качественного медицинского обслуживания, безопасности пациентов и успешной работы всего медицинского учреждения. Эффективная политика информационной безопасности позволяет не только предотвращать потенциальные угрозы, но и формировать культуру безопасного обращения с данными среди сотрудников, что в свою очередь делает больницу более устойчивой к вызовам цифровой эпохи.

**Использованные источники**

1. Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» (с изменениями и дополнениями).
2. Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных».
3. Постановление Оперативно-Аналитического центра при Президенте Республики Беларусь от 14.12.2018 № 66 «Об утверждении требований по обеспечению защиты информации».
4. ТКП 17.03-04-2019 (33150) «Информационные технологии и безопасность. Защита информации. Порядок проведения оценки соответствия».
5. ISO/IEC 27001:2022 — международный стандарт информационной безопасности.
6. NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations.
7. OWASP Foundation. "Top Ten Security Risks" (https://owasp.org/www-project-top-ten/).
8. Герасимов А.В., Сидорова Е.П. «Информационная безопасность организаций: угрозы, методы защиты, правовое регулирование» — Минск: БГУИР, 2021.
9. Кузнецов М.А., Соловьев Д.А. «Информационная безопасность: угрозы, защита, правовые аспекты» — М.: Бином, 2021.
10. Васильев А.А., Гаврилов С.П. «Кибербезопасность в здравоохранении» — СПб.: Питер, 2020.
11. Статья в журнале "Компьютерные системы и сети": Иванов И.И. «Современные угрозы информационной безопасности в медицинских учреждениях» // №4, 2023.