|  |
| --- |
| **МИНОБРНАУКИ РОССИИ**  федеральное государственное бюджетное образовательное  учреждение высшего образования  **«Национальный исследовательский университет «МЭИ»** |

|  |  |
| --- | --- |
| **Институт** | ИНЭИ |
| **Кафедра** | БИТ |

**КУРСОВАЯ РАБОТА**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Направление** | | | **10.03.01 «Информационная безопасность»** | | | | |
| (код и наименование) | | | | | | | |
| **Направленность (профиль)** | | | | | | | **БАС** |
|  | | | | | | | |
|  | | | | | | | |
| **Форма обучения** | | | | | **Очно-заочная** | | |
|  | (очная/очно-заочная/заочная) | | | | | | |
| **Тема:** | **Разработка программы аудита информационной безопасности** | | | | | | |
| **для медицинского центра.** | | | | | | | |
|  | | | | | | | |
|  | | | | | | | |
|  | | | | | | | |
| **Студент** | | **ИЭозс 43-22 Камчиев Б.А.** | | | | | |
| группа подпись фамилия и инициалы | | | | | | | |
| **Научный руководитель** | | | | **Доцент Писаренко И.В.** | | | |
| уч. степень должность подпись фамилия и инициалы | | | | | | | |
|  | | | | | |  | |
|  | | | | | | | |

Федеральное государственное бюджетное образовательное

учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

|  |  |  |  |
| --- | --- | --- | --- |
| Институт: | ИнЭИ | Кафедра: | БИТ |
| Направление подготовки/специальность: | | 10.03.01 Информационная безопасность | |

**ЗАДАНИЕ**

**на выполнение КП/КР по дисциплине**

**«**Аудит безопасности информационных систем**»**

|  |  |
| --- | --- |
| **Тема КП/КР:** | Разработка программы аудита информационной безопасности для медицинского центра. |
|  | |
| **Студент:** | Камчиев Бозулан Абдуллаевич |
|  | *(Фамилия, имя, отчество (при наличии) полностью)* |
| **Группа:** | ИЭозс-43-22 |
|  | *(номер учебной группы)* |

|  |
| --- |
| **Содержание задания:** |
| 1.Выбор темы КР |
| 2.Подготовка введения и листа задания на КР |
| 3.Разработка Главы 1 КР |
| 4.Разработка глав 2 и 3 КР |
| 5.Подготовка заключения и списка литературы |
| 6.Подготовка презентации и доклада к выступлению |
| *(вопросы, подлежащие изучению в соответствии с планируемыми результатами обучения,*  *заполняются руководителем КП/КР)* |

|  |  |  |
| --- | --- | --- |
| Руководитель |  | И.В. Писаренко |
|  | *(дата)* | (*Фамилия и инициалы*) |

|  |  |  |
| --- | --- | --- |
| Студент |  | Б.А. Камчиев |
|  | *(дата)* | (*Фамилия и инициалы*) |

Содержание

[Введение 4](#_Toc185111315)

[1 Теоретические основы аудита информационной безопасности в медицинских учреждениях. 5](#_Toc185111316)

[1.1 Понятие и цели аудита информационной безопасности. 5](#_Toc185111317)

[1.2 Нормативно-правовое регулирование в области ИБ медицинских учреждений 5](#_Toc185111318)

[1.3 Основные угрозы и риски информационной безопасности 5](#_Toc185111319)

[1.4 Виды аудита информационной безопасности: 6](#_Toc185111320)

[2 Разработка программы аудита информационной безопасности. 7](#_Toc185111321)

[2.1 Понятие и анализ Медицинского центра. 7](#_Toc185111322)

[2.2 Разработка программы аудита информационной безопасности для медицинского центра 8](#_Toc185111323)

[Заключение 14](#_Toc185111324)

[Список литературы 15](#_Toc185111325)

**Введение**

Информационная безопасность в медицинских учреждениях является критически важным аспектом в современном здравоохранении. Медицинские центры ежедневно обрабатывают огромные объемы конфиденциальной информации о пациентах, включая персональные данные, медицинские диагнозы и результаты исследований. Утечка или несанкционированный доступ к такой информации может привести к серьезным последствиям, включая нарушение прав пациентов, репутационный ущерб для медицинского учреждения и финансовые потери. В связи с этим, разработка эффективной программы аудита информационной безопасности является неотъемлемой частью обеспечения защиты медицинских данных.

Целью данной курсовой работы является Разработка программы аудита информационной безопасности для медицинского центра «Мидси».

Объект исследования: Информационная инфраструктура и процессы медицинского центра.

Предмет исследования: Процессы аудита информационной безопасности и методы ее обеспечения.

Для достижения поставленной цели необходимо решить следующие задачи:

* Провести анализ нормативной базы в области ИБ для медицинских учреждений.
* Изучить теоретические основы аудита ИБ.
* Провести анализ информационной инфраструктуры медицинского центра.
* Выявить основные угрозы и риски ИБ для медицинского центра.
* Разработать методологию и план проведения аудита ИБ.

1. **Теоретические основы аудита информационной безопасности в медицинских учреждениях.**
   1. **Понятие и цели аудита информационной безопасности.**

Аудит информационной безопасности **-** это комплексный процесс, направленный на оценку адекватности и эффективности мер защиты информации в организации. Он включает в себя проверку соответствия информационной системы требованиям законодательства, нормативных актов, стандартов и внутренних политик, а также идентификацию уязвимостей и потенциальных угроз безопасности. Основной целью аудита ИБ является предоставление руководству объективной и независимой оценки состояния информационной безопасности и рекомендаций по ее улучшению. Основные цели аудита ИБ включают:

* Выявление слабых мест и уязвимостей в системе ИБ.
* Оценка эффективности мер защиты информации.
* Проверка соответствия нормативным требованиям и стандартам.
* Предоставление рекомендаций по улучшению ИБ.
  1. **Нормативно-правовое регулирование в области ИБ медицинских учреждений**

Основные нормативные документы, регулирующие ИБ в медицинских учреждениях, включают:

* Федеральный закон №152-ФЗ “О персональных данных”.
* Приказ ФСТЭК России №17 “Об утверждении Требований о защите персональных данных”.
* Стандарт ISO 27001:2013 “Информационная безопасность. Системы менеджмента информационной безопасности. Требования”.
* Стандарт ISO/IEC 27799:2016 “Информационная безопасность в здравоохранении”.
  1. **Основные угрозы и риски информационной безопасности**
* Кибератаки (фишинг, DDoS, ransomware);
* Утечки данных (через инсайдеров или хакеров);
* Несанкционированный доступ к информации;
* Сбои оборудования и программного обеспечения;
* Недостаточная осведомленность персонала о правилах ИБ.
  1. **Виды аудита информационной безопасности:**
* Внутренний аудит:

Проводится сотрудниками медицинской организации для оценки ИБ изнутри.

* Внешний аудит:

Проводится независимой сторонней организацией.

* Аудит соответствия:

Проводится для проверки соответствия требованиям нормативных документов.

* Тематический аудит:

Фокусируется на конкретной области ИБ (например, управление доступом или сетевая безопасность).

1. **Разработка программы аудита информационной безопасности.**

**2.1 Понятие и анализ Медицинского центра.**

Медицинский центр — это многофункциональное медицинское учреждение, которое предоставляет широкий спектр медицинских услуг населению. В отличие от поликлиник или больниц, медицинские центры часто специализируются на предоставлении как амбулаторной, так и (иногда) стационарной помощи в различных областях медицины. Они могут быть как государственными, так и частными, и различаются по размеру, профилю и предоставляемым услугам. Организационная структура включает:

* Административный блок.
* Регистратуру.
* Диагностическое отделение.
* Отделение терапии.
* Хирургическое отделение.
* Лабораторию.
* Фармацевтический пункт.

Основные бизнес-процессы: запись на прием, проведение консультаций, диагностика, лечение, лабораторные исследования, хранение данных о пациентах.

Информационная система включает:

* Медицинскую информационную систему - система автоматизации документооборота для медицинских учреждений, в которой объединены система поддержки принятия врачебных решений, электронные медицинские карты пациентов, данные медицинских исследований в цифровой форме, данные мониторинга состояния пациента с медицинских приборов, средства общения между сотрудниками, финансовая и административная информация;
* Систему управления базами данных - программное обеспечение для создания и работы с базами данных, главная функция СУБД – это управление данными (которые могут быть как во внешней, так и в оперативной памяти);
* Серверы приложений и баз данных.
* Рабочие станции персонала - Рабочая станция медперсонала — это автоматизированное рабочее место, программно-аппаратный комплекс, который облегчает выполнение профессиональных обязанностей.
* Сетевое оборудование (маршрутизаторы, коммутаторы).

Анализ выявленных уязвимостей и рисков в существующей информационной инфраструктуре:

* Слабая парольная политика.
* Отсутствие сегментации сети.
* Недостаточное обновление программного обеспечения.
* Отсутствие многофакторной аутентификации.
* Недостаточная осведомленность персонала о правилах ИБ.

**2.2 Разработка программы аудита информационной безопасности для медицинского центра**

Цели и задачи программы аудита:

* Проверить соответствие требованиям 152-ФЗ и стандарту ISO 27001.
* Оценить текущий уровень ИБ.
* Выявить уязвимости и риски.
* Разработать рекомендации по улучшению ИБ.
* ISO/IEC 27001.
* Этот стандарт описывает требования к созданию, внедрению, поддержанию и улучшению системы управления информационной безопасностью (СУИБ). Он включает:
* Оценку рисков.
* Определение контекста организации.
* Разработку и внедрение политик и процедур.

ISO/IEC 27002.

Стандарт предоставляет рекомендации по контролю безопасности информации и описывает лучшие практики управления ИБ, включая:

* Политики безопасности
* Управление доступом.
* Обучение и повышение осведомленности.

На основе рассмотренной нормативно-правовой базы разработана программа аудита информационной безопасности для медицинского центра. Программа охватывает все необходимые этапы и процессы, обеспечивающие достижение целей аудита и повышение уровня ИБ в медицинском центре.

Основными целями программы аудита информационной безопасности (ИБ) являются:

1. Оценка соответствия

• Соответствие нормативным требованиям: Проверка выполнения требований законодательства, стандартов и нормативных актов в области ИБ (например, ФЗ-152, ISO/IEC 27001 и др.).

• Соблюдение внутренних политик: Оценка соответствия внутренним политикам и процедурам, установленным организацией.

2. Выявление уязвимостей

• Анализ уязвимостей: Идентификация слабых мест в системах, процессах и инфраструктуре, которые могут быть использованы злоумышленниками.

• Тестирование на проникновение: Проведение симуляций атак для проверки эффективности существующих мер безопасности.

3. Оценка рисков

• Идентификация угроз: Выявление потенциальных угроз, которые могут повлиять на безопасность информации и операционные процессы.

• Оценка уровня риска: Оценка вероятности возникновения угроз и их потенциального воздействия на организацию.

4. Улучшение контроля безопасности

• Оценка эффективности существующих мер: Анализ текущих средств контроля и их способности защищать информацию от угроз.

• Рекомендации по улучшению: Предоставление рекомендаций для повышения уровня безопасности и улучшения процессов управления ИБ.

Разработка методологии аудита:

Этапы: Планирование, сбор информации, анализ, тестирование, отчетность.

Методы: Опросы персонала, анализ документации, сканирование на уязвимости, тестирование на проникновение.

Определение области аудита:

* Все информационные системы медицинского центра.
* Процессы обработки персональных данных.
* Система управления доступом.
* Сетевая инфраструктура.
* Физическая безопасность серверной комнаты.

Разработка списка контрольных процедур и показателей для оценки эффективности информационной безопасности:

Управление доступом: Проверка парольной политики, прав доступа, журнала аудита.

Сетевая безопасность: Сканирование на уязвимости, анализ настроек межсетевого экрана, проверка IDS/IPS.

* + Защита данных;
  + Проверка наличия резервных копий;
  + Шифрования;
  + контроля доступа к базам данных.

Управление инцидентами: Оценка процессов обнаружения и реагирования на инциденты.

Оценка рисков: Анализ выявленных уязвимостей и их потенциального воздействия.

Определение частоты проведения аудита: Внешний аудит – 1 раз в год, внутренние аудиты – ежеквартально.

Разработка плана аудита: Подготовка и планирование, сбор информации и анализ документации, проведение сканирования на уязвимости и тестирования, анализ результатов и разработка отчета.

Определение инструментов и ресурсов для проведения аудита:

Программное обеспечение и квалифицированный персонал: аудитор ИБ, специалист по безопасности, сетевой администратор.

Существует вероятность возникновения следующих нарушений информационной безопасности:

* + получение неправомерного доступа к информации, другими словами, нарушение конфиденциальности;
  + утрата сведений, вызванная разрушением носителя информации или стиранием данных;
  + внесение изменений при прямом доступе к базе данных или через интерфейс системы;
  + отказ функционала, связанный с получением доступа к информации;
  + получение доступа к базе данных – полное или частичное;
  + некорректное функционирование информационной системы вследствие несанкционированного изменения модулей.

Способы усиления защиты сведений в информационных системах медицинских организаций.

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

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.

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.

Перечень технических 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.

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.

Безопасность данных должны быть реализована на всех уровнях работы медицинской информационной системы: сведения о пациентах; данные о персонале; информация о медучреждении; сведения о системе здравоохранения, как в государственных, так и в частных организациях.

**Заключение**

В результате курсовой работы была разработана программа аудита информационной безопасности для медицинского центра. Программа учитывает специфику деятельности медицинского учреждения, соответствует требованиям нормативных документов и включает в себя методику, план и контрольные процедуры для проведения аудита.

Реализация разработанной программы аудита позволит выявить уязвимости и риски ИБ, оценить эффективность существующих мер защиты и разработать рекомендации по их улучшению. Это будет способствовать повышению уровня информационной безопасности медицинского центра и защите конфиденциальной информации пациентов.

**Список литературы**

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ
2. Приказ ФСТЭК России №17 “Об утверждении Требований о защите персональных данных”.
3. Стандарт ISO 27001:2013 “Информационная безопасность. Системы менеджмента информационной безопасности. Требования”.
4. Стандарт ISO/IEC 27799:2016 “Информационная безопасность в здравоохранении”.
5. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов/ Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024.— 277 с.— (Высшее образование). — ISBN 978-5-534-16450-3.
6. Аудит информационной безопасности. Учебное пособие 4-е издание, стереотипное, автор В. И. Аверченков
7. Информационная безопасность медицинской организации. (Специалитет). Учебное пособие. автор Сергей Дмитриенвич Гусев.