Организация аудита значимого объекта критической информационной инфраструктуры

УКОРОЧЕННАЯ ВЕРСИЯ ПРЕЗЕНТАЦИИ

Объект и предмет исследования

Объектом исследования является информационная инфраструктура кардиологического отделения «Первой Университетской Клиники».

Предметом исследования являются подходы и процессы проведения аудита значимых объектов критической информационной инфраструктуры.

Цели и задачи исследования

Цель работы заключается в определении текущего уровня безопасности кардиологического отделения «Первой Университетской Клиники» и выявлении перечня мер и мероприятий, необходимых для обеспечения соответствия требованиям ФЗ № 187 и другой регламентирующей документации. Для достижения указанной цели предполагается решить следующие задачи:

1. Исследовать теоретические аспекты вопроса проведения аудита информационной безопасности значимых объектов критической информационной инфраструктуры.
2. Провести аудит ИТ-инфраструктуры в контексте анализа защищенности значимых объектов критической информационной инфраструктуры кардиологического отделения «Первой Университетской Клиники», обрабатывающего персональные данные.
3. Разработать модели нарушителя и актуальных угроз безопасности объектов критической информационной инфраструктуры кардиологического отделения «Первой Университетской Клиники».
4. Выявить критические процессы и определить значимые объекты критической информационной инфраструктуры кардиологического отделения «Первой Университетской Клиники».
5. Провести диагностический аудит и описать ключевые аспекты проведения инструментального аудита значимого объекта критической информационной инфраструктуры.
6. Получить результаты предварительных испытаний предложенных по результатам проведения аудита мер защиты информации в целях нейтрализации выявленных актуальных угроз.

Основные этапы проведения аудита ИБ объектов критической информационной инфраструктуры

Инициирование аудита	• Назначение ответственных и руководителя группы аудиторов объекта КИИ • Формирование группы аудиторов • Определение целей, границ проведения аудита, критериев • Разработка плана проведения аудита объекта КИИ
Подготовка к обследованию	• Подготовка программы (плана) обследования • Распределение заданий в группе по аудиту объекта КИИ • Подготовка рабочих документов
Обследование объекта	• Проведение вводного совещания • Проведение диагностического обследования • Проведение инструментального обследования • Проведение тестирования на проникновение • Сбор и проверка информации • Проведение завершающего совещания
Разработка отчета	• Подготовка отчета, описывающего текущее положение дел • Подготовка отчета с рекомендациями • Утверждение и рассылка отчета по аудиту объекта КИИ
Завершение аудита	• Разъяснение спорных вопросов • Проведение итогового совещания, разъяснение рекомендаций по итогам аудита объекта КИИ

Подтверждение категории выявленных объектов критической информационной инфраструктуры кардиологического отделения

По результатам оценки в рамках проведения аудита было подтверждено:

1. Отсутствие необходимости отнесения корпоративной сети к объектам критической информационной инфраструктуры медицинской организации.
2. ИС, связанные с обслуживанием клиентов и сотрудников, а также АСУ по работе с оборудованием и пожаротушением отнесены к 3 категории значимости.

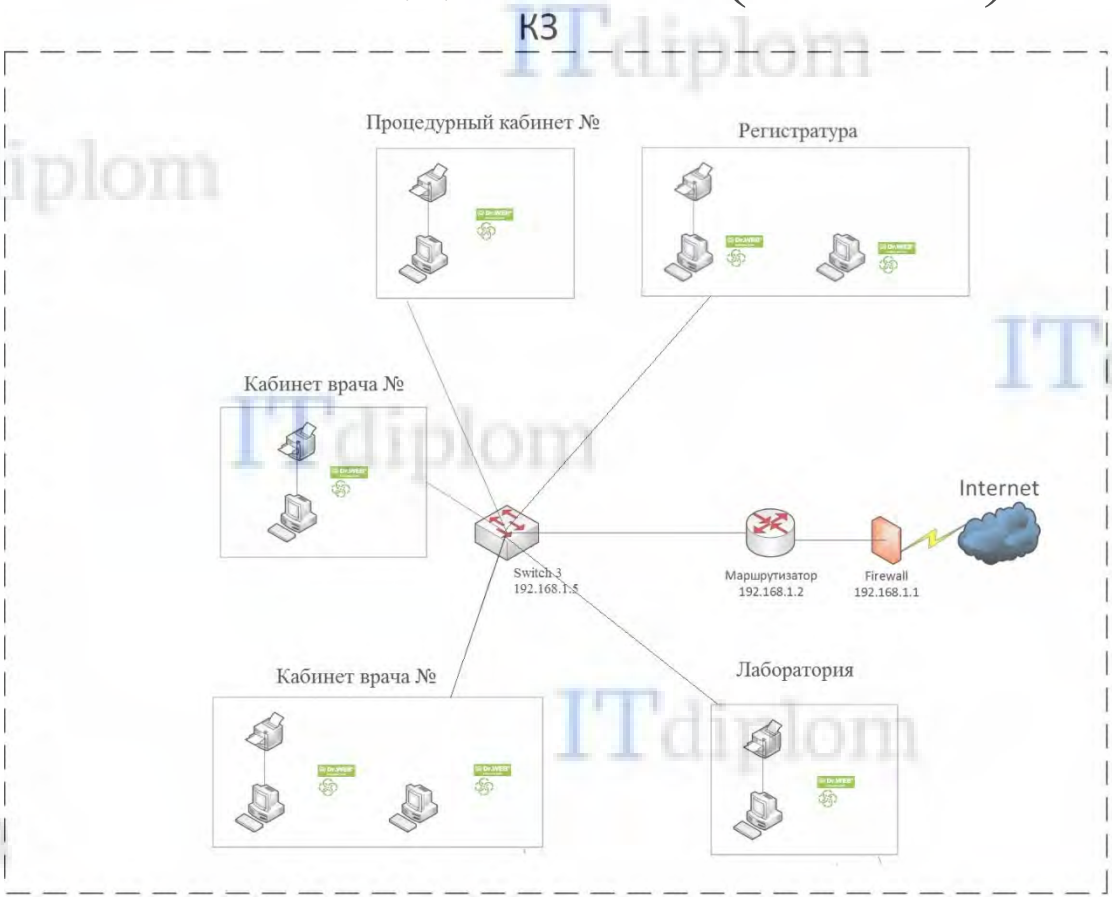
Для 3 класса значимости предусмотрен следующий перечень мер защиты:

- Идентификация и аутентификация.
- Управление доступом.
- Защита машинных носителей информации.
- Аудит безопасности.
- Антивирусная защита.
- Обеспечение целостности.
- Обеспечение доступности.
- Защита технических средств и систем.
- Защита информационной (автоматизированной) системы и ее компонентов.
- Планирование мероприятий по обеспечению безопасности.
- Управление конфигурацией.
- Управление обновлениями программного обеспечения.
- Реагирование на компьютерные инциденты.
- Обеспечение действий в нештатных ситуациях.
- Информирование и обучение персонала.

Оценка оптимальности существующего комплекса мер обеспечения защиты (для угроз с применением программно-аппаратных средств)

Наименование угрозы	Меры по противодействию угрозе	
	Технические и физические	Организационные
Угрозы значимых объектов критической информационной инфраструктуры с применением программных и программно-аппаратных средств		
Угроза внедрения программных "закладок" и "вирусов"	СрЗИ НСД «Secret Net», ABC. Dr.Web Enterprise Security Suite, АПК «Аргус»	Инструкции персоналу, ограничение использования внешних носителей, ведение Журнала учета носителей и использования сети Интернет, установка сертифицированного ПО
Угроза незаконного получения паролей и других реквизитов разграничения доступа с дальнейшим их использованием	СрЗИ НСД «Secret Net», АПК «Аргус»	Инструкции персоналу, периодическая смена паролей, ограничение использования внешних носителей, установка сертифицированного ПО, соблюдение порядка использования паролей
Угроза реализации скрытого канала передачи данных	СрЗИ НСД «Secret Net»,	Первичная и периодическая проверка сотрудников СБ
Угроза перехвата конфиденциальной информации по сети	СрЗИ НСД «Secret Net», АПК «Аргус»	Инструкции персоналу

Выработка рекомендаций в рамках проведенного аудита кардиологического отделения (2 этаж)



Результаты выполненной работы

1. Исследованы теоретические аспекты вопроса проведения аудита информационной безопасности значимых объектов критической информационной инфраструктуры.
2. Проведен аудит ИТ-инфраструктуры в контексте анализа защищенности значимых объектов критической информационной инфраструктуры кардиологического отделения «Первой Университетской Клиники», обрабатывающего персональные данные.
3. Разработаны модели нарушителя и актуальных угроз безопасности объектов критической информационной инфраструктуры кардиологического отделения «Первой Университетской Клиники».
4. Выявлены критические процессы и определены значимые объекты критической информационной инфраструктуры кардиологического отделения «Первой Университетской Клиники».
5. Проведен диагностический аудит и описаны ключевые аспекты проведения инструментального аудита значимого объекта критической информационной инфраструктуры.
6. Получены результаты предварительных испытаний предложенных по результатам проведения аудита мер защиты информации в целях нейтрализации выявленных актуальных угроз.

Полученные результаты могут быть использованы коммерческими организациями и государственными предприятиями для выявлении перечня мер и мероприятий, учитывающих требования Федеральных законов и других нормативных документов в отношении обработки данных на субъектах критической информационной инфраструктуры.