СОДЕРЖАНИЕ

[Введение 3](#_Toc29152687)

[1. Анализ основных угроз информационной безопасности сетевой инфраструктуры организации 6](#_Toc29152688)

[1.1. Уязвимости сетевой инфраструктуры 7](#_Toc29152689)

[1.1.1 Стандарт CVSS 8](#_Toc29152690)

[1.1.2 Базы уязвимостей 14](#_Toc29152691)

[1.1.3 Уязвимости, способствующие удаленной компрометации узла 23](#_Toc29152692)

[1.2. Эксплойты 23](#_Toc29152693)

[1.3. Тестирование на проникновение 25](#_Toc29152694)

[1.3.1 Сбор информации о системе 26](#_Toc29152695)

[1.3.2 Проникновение в целевую систему 27](#_Toc29152696)

[1.3.3 Осуществление несанкционированных действий 27](#_Toc29152697)

[1.3.4 Сокрытие следов несанкционированного доступа 27](#_Toc29152698)

1.4 Выводы 28

[2. Оценка защищенности и выбор мер защиты сетевой инфраструктуры организации 28](#_Toc29152699)

[2.1. Методики оценки защищенности компьютерной сети 28](#_Toc29152702)

[2.1.1 Качественные методики оценки защищенности 28](#_Toc29152703)

[2.1.2 Количественные методики оценки защищенности 32](#_Toc29152707)

[2.1.3 Смешанные методики оценки защищенности 35](#_Toc29152708)

[2.2. Концепция графов атак 39](#_Toc29152709)

[2.3. Показатели защищенности 41](#_Toc29152710)

[2.3.1 Базовые показатели 42](#_Toc29152714)

[2.3.2 Показатели на основе графов атак 43](#_Toc29152715)

[2.4 Методики выбора защитных мер на основе графов атак 45](#_Toc29152716)

[2.4.1 Методика поддержки принятия решений, интегрированная в IDS 45](#_Toc29152717)

[2.4.2 Методики на основе теории игр 46](#_Toc29152718)

[2.4.3 Методики на основе количества достижимых узлов 46](#_Toc29152719)

[2.4.4 Методика на основе показателя процента компрометации сети (NCP) 47](#_Toc29152720)

[2.5 Интегральные показатели 48](#_Toc29152721)

[2.6 Выводы 48](#_Toc29152722)

[3. Разработка методик оценки защищенности и выбора защитных 51](#_Toc29152723)

[3.1 Показатели защищенности узлов сетевой инфраструктуры 51](#_Toc29152724)

[3.2 Методика оценки защищенности сетевой инфраструктуры 54](#_Toc29152725)

[3.3 Методика выбора защитных мер 56](#_Toc29152726)

[4 Реализация системы оценки защищенности и выбора защитных мер 60](#_Toc29152727)

[4.1 Архитектура системы оценки защищенности и выбора защитных мер 61](#_Toc29152728)

[Заключение 65](#_Toc29152729)

[Список использованных источников 67](#_Toc29152730)

[Приложение А 71](#_Toc29152731)