СОДЕРЖАНИЕ

[Введение 3](#_Toc29292193)

[1. Анализ основных угроз информационной безопасности сетевой инфраструктуры организации 6](#_Toc29292194)

[1.1. Уязвимости сетевой инфраструктуры 7](#_Toc29292195)

[1.1.1 Стандарт CVSS 8](#_Toc29292196)

[1.1.2 Базы уязвимостей 14](#_Toc29292197)

[1.1.3 Уязвимости, способствующие удаленной компрометации узла 22](#_Toc29292198)

[1.2. Эксплойты 23](#_Toc29292199)

[1.3. Тестирование на проникновение 25](#_Toc29292200)

[1.3.1 Сбор информации 28](#_Toc29292201)

[1.3.2 Проникновение на целевой узел 29](#_Toc29292202)

[1.4. Выводы 30](#_Toc29292203)

[2. Оценка защищенности и выбор мер защиты сетевой инфраструктуры организации 32](#_Toc29292204)

[2.1. Методики оценки защищенности компьютерной сети 32](#_Toc29292207)

[2.1.1 Качественные методики оценки защищенности 32](#_Toc29292208)

[2.1.2 Количественные методики оценки защищенности 36](#_Toc29292212)

[2.1.3 Смешанные методики оценки защищенности 39](#_Toc29292213)

[2.2 Концепция графов атак 43](#_Toc29292214)

[2.3 Показатели защищенности 45](#_Toc29292215)

[2.3.1 Базовые показатели 46](#_Toc29292219)

[2.3.2 Базовые показатели на основе графов атак 47](#_Toc29292220)

[2.4 Методики выбора защитных мер на основе графов атак 49](#_Toc29292221)

[2.4.1 Методика поддержки принятия решений, интегрированная в IDS 49](#_Toc29292222)

[2.4.2 Методики на основе теории игр 50](#_Toc29292223)

[2.4.3 Методики на основе количества достижимых узлов 51](#_Toc29292224)

[2.4.4 Методика на основе показателя процента компрометации сети (NCP) 51](#_Toc29292225)

[2.5 Интегральные показатели 52](#_Toc29292226)

[2.6 Выводы 53](#_Toc29292227)

[3. Разработка методик оценки защищенности и выбора защитных 55](#_Toc29292228)

[3.1 Показатели защищенности узлов сетевой инфраструктуры 55](#_Toc29292229)

[3.2 Методика оценки защищенности сетевой инфраструктуры 58](#_Toc29292230)

[3.3 Методика выбора защитных мер 59](#_Toc29292231)

[4 Реализация системы оценки защищенности и выбора защитных мер 65](#_Toc29292232)

[4.1 Архитектура системы оценки защищенности и выбора защитных мер 65](#_Toc29292233)

[Заключение 70](#_Toc29292234)

[Список использованных источников 72](#_Toc29292235)

[Приложение А 76](#_Toc29292236)