

242433 Совершенствование методики мониторинга угроз с помощью SIEM-системы

Введение 2

1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ МЕНЕДЖМЕНТА УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 4

1.1. Правовая характеристика угроз информационной безопасности 4

1.2. Особенности выявления и реагирования на угрозы в области информационной безопасности 17

2 СРАВНИТЕЛЬНЫЙ АНАЛИЗ АКТУАЛЬНЫХ МОДЕЛЕЙ И МЕТОДОВ ВЫЯВЛЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 28

2.1 Методики выявления угроз ИБ 28

2.1.1 Модели качественного и количественного анализа угроз и рисков информационной безопасности 28

2.1.2 Модели качественного и количественного анализа угроз и рисков информационной безопасности систем по методике OUSTAVE 29

2.1.3 Риск-модель CRAMM30

2.1.4 Методика выявления угроз в соответствии с требованиями ФСТЭК 31

2.2 Метод анализа иерархий 34

2.3 SIEM-система как инструмент противодействия угрозам ИБ 39

3 СОВЕРШЕНСТВОВАНИЕ МЕТОДИКИ МОНИТОРИНГА УГРОЗ ИБ С ИСПОЛЬЗОВАНИЕМ SIEM-СИСТЕМЫ 56

**3.1 Проблемы существующих методик мониторинга угроз ИБ
56**

**3.2 Рекомендации и предложения по совершенствованию
методик мониторинга угроз с помощью SIEM-системы 60**

**3.2.1 Разработка рекомендаций и предложений на основе сводки
полученных результатов 60**

3.2.2 Настройка оповещений 69

Telegram bot 69

Discord bot 71

Email 74

**3.2.3 Экономическая оценка по внедрению рекомендаций и
предложений 76**

**3.2.4 Выбор и обоснование методики расчёта экономической
эффективности 83**

**3.2.5 Расчёт показателей экономической эффективности проекта
85**

Заключение 91

Список использованных сокращений 93