

232437 Методы анализа защищенности информационных систем и расследования инцидентов на основе технологий обработки информации OSINT

Аннотация	7
Введение	8
Перечень терминов, обозначения и сокращений	11
1 Анализ нормативных требований по оценке защищенности информационных систем и расследованию инцидентов	13
1.1 Нормативные документы в сфере оценки защищенности информационных систем с информацией ограниченного доступа	12
1.2 Нормативные документы в сфере оценки защищенности информационных систем с общедоступной информацией	16
1.3 Выводы	18
2 Анализ технологий сбора информации из открытых источников OSINT	19
2.1 Назначение и цели OSINT	19
2.2 Структура OSINT	22
2.3 Технологии OSINT	26
2.4 Методы пассивного сбора информации	29
2.5 Методы активного сбора информации (тестирование на проникновение)	30
2.6 Инструменты	33
2.7 Применение искусственного интеллекта	35
2.8 Геопространственная разведка	37
2.9 Форензика	41

2.10	Выводы	42
3	Оценка защищенности информационных систем с использованием технологии OSINT	44
3.1	Основные этапы исследования защищенности информационных систем с использованием OSINT	44
3.2	Рекомендации по использованию OSINT при расследовании инцидентов и анализе информационных систем	47
3.3	Анализ персоны	52
3.4	Анализ сайта компании	55
3.5	Расследование инцидента	56
3.6	Конкурентная разведка	59
3.7	Выводы	62
4	Предложения по включению в курс подготовки бакалавров по направлению 09.03.03 «Прикладная информатика» раздела обучения технологиям OSINT	63
4.1	Цели обучения	63
4.2	Программа обучения	63
4.3	Учебно-методическое обеспечение	66
	Заключение	67
	Список использованных источников	69