

Оглавление

Введение.....	3
1. Анализ состояния предметной области. Постановка задач исследования.....	7
1.1. Анализ нормативно-правовой базы, регламентирующей подходы к оценке угроз компьютерных атак....	7
1.1.1. Определение базового набора мер защиты информации.....	10
1.1.2. Адаптация базового набора мер защиты информации.....	18
1.1.3. Уточнение адаптированного базового набора мер защиты информации.....	19
1.1.4. Дополнение уточнённого адаптированного базового набора мер защиты информации.....	24
1.1.5. Существующие ограничения Методики ФСТЭК России.....	24
1.2. Анализ международных методик, используемых для оценки угроз компьютерных атак.....	26
1.2.1. Методология IT-Grundschutz.....	26
1.2.2. Ограничения методологии IT-Grundschutz.....	35
1.2.3. Методология ISO 2700x.....	36
1.2.4. Ограничения методологии ISO.....	43
1.3. Анализ научных подходов к определению и прогнозированию компьютерных атак.....	44
1.4. Постановка задач исследования.....	49
2. Разработка математической модели принятия решения нарушителем о проведении компьютерной атаки и математической модели, описывающей динамику компьютерной атаки во времени.....	53
2.1. Базовые принципы и подходы к построению математических моделей, описывающих принятие решения нарушителем о проведении компьютерной атаки и ее динамику.....	53
2.2. Разработка математической модели принятия решения нарушителем о проведении компьютерной атаки.....	56
2.2.1. Функция ожидаемой полезности компьютерной атаки.....	56
2.2.2. Анализ функции ожидаемой полезности.....	58
2.2.3. Вероятность достаточности ожидаемой полезности..	60
2.2.4. Обоснование выбора источников первичной информации для расчета ожидаемой полезности от киберпреступления.....	61

2.2.5. Пример оценивания вероятности принятия решения преступником о проведении компьютерной атаки	64
2.2.6. Анализ результатов	67
2.3. Разработка математической модели, описывающей динамику возможности реализации компьютерной атаки во времени	68
2.4. Подтверждение адекватности математической модели динамики распространение компьютерной атака на примере компьютерной атаки, реализованной с помощью вредоносного программного обеспечения Wanna-Cry	77
2.4.1. Динамика реализации КА	77
2.4.2. Математическое обоснование выбора аппроксимирующей функции методом наименьших квадратов	81
2.5. Экспериментальные исследования динамики развития компьютерной атаки	83
2.5.1. Описание экспериментального стенда	83
2.5.2. Методика проведения натурального моделирования компьютерной атаки	85
2.5.3. Анализ результатов моделирования динамики развития компьютерной атаки	87
2.5.4. Результаты аппроксимации экспериментальной зависимости числа зараженных узлов от времени	92
2.6. Разработка рекомендаций для оценивания параметров математических моделей, описывающих динамику компьютерной атаки	94
2.6.1. Этапы реализации компьютерной атаки	94
2.6.2. Методы компьютерной атаки	99
2.6.3. Выбор характеристик компьютерной атаки, влияющих на возможность ее реализации	102
2.6.4. Выбор параметров функции изменения возможности реализации компьютерной атаки во времени	103
2.6.5. Обоснование выбора источников первичной информации для расчета возможности реализации метода компьютерной атаки	104
2.6.6. Оценка адекватности модели проведения компьютерной атаки на примере компьютерной атаки, реализованной с помощью вредоносного программного обеспечения Petya ..	106
2.6.7. Итоги анализа математической модели развития компьютерной атаки	110
2.7. Выводы	112

3. Разработка методики прогнозирования динамики вероятности проведения компьютерной атаки, основанной на использовании предложенных математических моделей, и подтверждение ее работоспособности	113
3.1. Анализ общедоступных источников информации о компьютерных атаках с точки зрения достаточности хранимой в них информации для идентификации параметров разработанных математических моделей компьютерной атаки и оценки их адекватности	114
3.2. Модель нарушителя и ее влияние на компьютерную атаку	117
3.3. Методика оценивания параметров функции прогнозирования динамики компьютерной атаки	118
3.4. Пример практического использования методики прогнозирования динамики компьютерной атаки, основанной на использовании предложенных математических моделей	120
3.5. Выводы	129
Заключение	131
Список сокращений	132
Литература	134
Приложение А. Присвоение категории значимости объектам критической информационной инфраструктуры в соответствии с показателями критериев значимости	151
Приложение В. Уровни возможностей нарушителей по реализации угроз безопасности информации	157
Приложение С. Оценка ущерба от различных сценариев негативных последствий инцидентов информационной безопасности	161
Приложение D. Научные подходы, используемые для определения и прогнозирования компьютерных атак	163
Приложение Е. Расчет тяжести наказания за преступления	197
Приложение F. Методы компьютерных атак, обсуждаемые в сети DarkNet	203
Приложение G. Анализ общедоступных источников статистической информации о компьютерной атаке	208
Приложение H. Описание ПАК Ampire	215