

33428 Установление авторства вредоносного программного обеспечения в подсистеме компьютерных инцидентов

Введение 3

1 Анализ задачи установления авторства вредоносного программного обеспечения в подсистеме компьютерных инцидентов 5

1.1 Инциденты информационной безопасности и их роль в информационно-телекоммуникационных системах 5

1.1.1 Классификация инцидентов информационной безопасности 5

1.1.2 Принципы формирования систем обнаружения инцидентов 7

1.2 Методы и способы обнаружения инцидентов информационной безопасности 7

1.2.1 Основные угрозы информационной безопасности 8

1.2.2 Методы выявления инцидентов информационной безопасности 15

1.3 Описание существующих технологий и их составляющих (технологических этапов, процессов, процедур, действий и т.п.) направленных на установление авторства ВПО (неформальное описание существующей практики по атрибуции ВПО) 17

1.3.1 Признаки ВПО и характеристика методов их распознавания в процессе атрибуции 17

1.3.2 Обработка исполняемых файлов спецификации PE 22

1.3.3 Функциональная модель системы установления авторства ВПО 22

1.3.4 Описание методов кластеризации ВПО 22

Динамические системы 29

Clique Graphs	30
1.3.5 Нейросетевая атрибуция ВПО	32
2 Разработка алгоритма установления авторства вредоносного программного обеспечения в подсистеме компьютерных инцидентов).	35
2.1 Формальная постановка задачи разработки алгоритма установления авторства вредоносного программного обеспечения	35
2.2 Определение методических, алгоритмических и технологических решений в области построения этапов, процессов, процедур и т.д. современной технологии атрибуции ВПО	36
2.2.1 Процедура идентификации ВПО в исполняемых файлах	36
2.2.2 Обобщенный алгоритм стохастической структурной атрибуции ВПО	42
2.2.3 Предложения по применению решений по атрибуции ВПО	46
2.2.4 Оценка эффективности предлагаемых решений	51
3 Особенности реализации алгоритма установления авторства вредоносного программного обеспечения в подсистеме компьютерных инцидентов.	56
3.1 Практическая реализация установления авторства вредоносного программного обеспечения в подсистеме компьютерных инцидентов	56
3.1.1 Возможности технологии Snort как средства установления авторства вредоносного программного обеспечения в подсистеме компьютерных инцидентов	56

3.1.2 Разработка виртуального модуля для интернета вещей, с использованием анализа трафика при помощи нейросети, позволяющего находить вторжения и атаки и сохранять данные об авторах вредоносного программного обеспечения 59

3.2 Экономическая эффективность внедрения виртуального модуля 70

3.2.1 Расчет трудозатрат и составление сметы затрат на выполнение проекта 71

3.2.2 Определение численности исполнителей 74

3.2.3 Разработка бизнес-плана и составление календарного графика выполнения проекта. 76

3.2.4 Описание методики расчет экономических показателей 81

3.2.5 Расчет показателей экономической эффективности 84

Заключение 88

Список использованных источников 90

ПРИЛОЖЕНИЕ 1. ДИАГРАММА ИСПОЛЬЗУЕМЫХ В ПРОЕКТЕ КЛАССОВ ИЗ БИБЛИОТЕКИ «PE-IMAGE-FOR-DELPHI» 93

ПРИЛОЖЕНИЕ 2. ФРАГМЕНТ ЛИСТИНГА ПРОГРАММНЫХ МОДУЛЕЙ 94