

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет радіоелектроніки і телекомунікацій

Захист інформації

Пояснювальна записка

до магістерської роботи
магістр

на тему: Дослідження засобів мережевого захисту та підвищення їх ефективності
на основі синтаксичного аналізу трафіку

Виконав: студент 5 курсу, групи РТ – 713м
напряму підготовки (спеціальності)

7.17010201 Системи технічного захисту
інформації, автоматизація її обробки

Аллянов М.О.

Керівник: доц. Романенко С.М.

Консультант: доц. Воскобойник В.О.

Рецензент _____

(прізвище та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет Радіoeлектроніки та телекомунікацій
Кафедра Захисту інформації
Спеціальність 7.17010201 Системи технічного захисту інформації, автоматизація її обробки

ЗАТВЕРДЖУЮ
Завідувач кафедри Карпуков Л.М.

« ____ » _____ 20__ р.

ЗАВДАННЯ

На магістерську роботу студента групи РТ-713м ОКР магістр _____
Аллянов Максим Олексійович
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Дослідження засобів мережевого захисту та підвищення їх ефективності на основі синтаксичного аналізу трафіку
затверджена наказом ЗНТУ від « ____ » 2018 р. № ____

2. Термін подання студентом закінченого проекту (роботи) « ____ » грудня 2018 р.

3. Вихідні дані для проекту (роботи) Підвищити ефективність існуючих засобів мережевого захисту на основі методу синтаксичного аналізу трафіку з метою покращення захищеності інформації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які належить розробити) Дослідження методів обходу засобів мережевого захисту шляхом тунелювання прикладних протоколів; розробка алгоритму синтаксичного аналізу трафіку.

5. Перелік графічного матеріалу Інтеграція синтаксичного аналізатора трафіку з МЕ для підвищення ефективності захисту;

Загальна схема взаємодії через тунель;

Залежність підвищення ефективності МЕ від виду тунелювання;

6. Перелік програмних продуктів, які належить використати в процесі розроблення проекту (роботи) Microsoft Office Word, Adobe Photoshop

7. Консультування проекту (роботи), із зазначенням розділів

Розділ	Консультант	Завдання видав		Завдання прийняв	
		підпис	дата	підпис	дата
Основна частина	Романенко С.М.				
Економічна частина					
Охорона праці					
Нормоконтроль	Нікуліщев Г.І.				

8. Дата, коли видано завдання « 03 » вересня 2018 р.

Керівник

(підпис)

Завдання прийняв до виконання

(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1.	Складання та затвердження ТЗ, підбір літератури	03.09 - 10.09.2018	
2.	Опис засобів мережевого захисту	11.09 - 02.10.2018	
3.	Моделювання протоколу мережевої взаємодії	03.10 - 22.10.2018	
4.	Моделювання лексикографічного протоколу мережевої взаємодії	23.10 - 03.11.2018	
5.	Реалізація аналітичної моделі мережевої взаємодії	04.11 - 09.11.2018	
6.	Розробка методики ефективності засобів мережевого захисту	09.11 - 15.11.2018	
7.	Розробка метода синтаксичного аналізу трафіку	16.11 - 18.11.2018	
8.	Розробка економічної частини	19.11 - 21.11.2018	
9.	Розробка заходів з охорони праці	22.11 - 28.11.2018	
10.	Оформлення графічної частини	29.11 - 03.12.2018	
11.	Оформлення пояснювальної записки	04.12 - 06.12.2018	

Завідувач кафедри

(підпис)

Керівник

(підпис)

Студент

(підпис)

РЕФЕРАТ

ПЗ: 103 с., 6 рис., 14 табл., 15 источников.

Цель магистерской работы – повышение эффективности существующих средств сетевой защиты посредством применения метода синтаксического анализа трафика с использованием контекстно-свободных грамматик.

Исследованы методы обхода средств сетевой защиты, основанные на туннелировании протоколов; предложен подход к оценке повышения эффективности средств сетевой защиты при обнаружении туннелирования.

Предложен алгоритм синтаксического анализа трафика согласно описаниям протоколов на специализированном языке и методика повышения эффективности средств сетевой защиты с применением этого алгоритма.

ТУННЕЛИРОВАНИЕ ПРОТОКОЛОВ, СРЕДСТВА СИНТАКСИЧЕСКОГО АНАЛИЗА ТРАФИКА, ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ, ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СЕТЕВОГО ЭКРАНА

СОДЕРЖАНИЕ

Введение.....	8
1. Обход средств сетевой защиты посредством туннелирования протоколов.....	11
1.1 Обход сетевой защиты путем туннелирования протоколов.....	11
1.1.1 Понятие туннелирования протоколов.....	11
1.1.2 Методы обхода средств сетевой защиты путем туннелирования протоколов.....	14
1.1.3 Методы обнаружения туннелирования протоколов.....	19
1.2 Повышение эффективности средств сетевой защиты путем предотвращения туннелирования.....	23
1.2.1 Причины снижения эффективности средств защиты при применении туннелирования.....	23
1.2.2 Метод синтаксического анализа в обнаружении туннелирования протоколов.....	26
1.3 Цель и задачи моделирования протокола сетевого взаимодействия.....	40
1.4 Лексикографическая модель протокола сетевого взаимодействия.....	40
1.5 Грамматика протокола сетевого взаимодействия.....	43
1.6 Выводы к главе.....	44
2. Средства синтаксического анализа трафика и их применение для обнаружения туннелирования протоколов в компьютерных сетях.....	45
2.1 Реализация аналитической модели сетевого взаимодействия с учетом ограничений, установленных требованиям к эффективности.....	45
2.2 Специализированный язык описания сетевого взаимодействия по протоколу.....	48
2.2.1 Общая структура описания протокола.....	48
2.2.2 Основные понятия языка.....	49
2.2.3 Лексические единицы языка.....	50
2.2.4 Операторы языка.....	51

2.3 Алгоритм синтаксического анализа дампов трафика при сетевом взаимодействии по прикладным протоколам.....	53
2.4 Выводы к главе	62
3. Повышение эффективности средств защиты посредством синтаксического анализа трафика.....	64
3.1 Методика повышения эффективности средств сетевой защиты на основе синтаксического анализа трафика.....	64
3.2 Прототип программного средства, реализующий метод синтаксического анализа трафика для повышения эффективности межсетевого экрана.....	66
3.3 Результаты экспериментальных исследований.....	68
3.4 Выводы к главе.....	70
4. Охрана труда и безопасность в чрезвычайных ситуациях.....	71
4.1 Анализ потенциальных опасностей.....	71
4.2 Мероприятия по обеспечению безопасности.....	72
4.3 Мероприятия по производственной санитарии и гигиены труда.....	74
4.4 Мероприятия по пожарной безопасности.....	79
4.5 Мероприятия по гражданской обороне.....	81
4.6 Вывод к главе.....	85
5. Организационно-экономические расчеты.....	87
5.1 Планирование научно-исследовательских работ.....	87
5.1.1 Определение трудоемкости и продолжительности НИР.....	87
5.1.2 Составление сетевого графика.....	88
5.2 Определение затрат на проведение НИР.....	94
5.3 Расчет экономической эффективности НИР.....	96
5.4 Использование компьютерных технологий для решения экономических задач.....	98
Выводы.....	101
Перечень ссылок.....	102

ПЕРЕЧЕНЬ ССЫЛОК

1. Рудина, Е.А. Спецификация сетевых протоколов с использованием декларативного языка описания. / Е.А. Рудина // Проблемы информационной безопасности. Компьютерные системы - СПб.: Изд-во Политехи, ун-та, 2012. - № 2 - С.69-75.
2. Рудина, Е.А. Подход к анализу клиент-серверного взаимодействия на основе декларативного описания сетевого протокола / С.С. Корт, Е.А. Рудина // «Проблемы информационной безопасности. Компьютерные системы». - СПб.: Изд-во Политехи, ун-та, 2011., - № 4, С.27-39.
3. Рудина, Е.А. Обобщенное представление сетевых протоколов. / Е.А. Рудина // «Проблемы информационной безопасности. Компьютерные системы». - СПб.: Изд-во Политехи, ун-та, 2008. - № 4, С.56-60.
4. Рудина, Е.А. Контекстно-детерминированная идентификация прикладных протоколов в дампах сетевого трафика. / Е.А. Рудина // Сб.материалов Международной молодежной конференции «Информационные системы и технологии». – М:Изд-во ЦРГОПиИТ, 2012. - С.94-96.
5. Рудина, Е.А. Вычислительные сети: лабораторный практикум / С.С. Корт, Е.А. Рудина. - СПб.: Изд-во Политехи, ун-та, 2011. - 188 с.
6. Рудина, Е.А. Поиск вариаций в полях сетевых пакетов по декларативному описанию протоколов. / А.В. Шумов, Е.А. Рудина // Сб.Материалов «XXXVIII Недели науки СПбГПУ», СПб.: Изд-во Политехи, ун-та, 2009. - С. 171-172.
7. Тель, Ж. Введение в распределенные алгоритмы //Ж. Тель,.В.А. Захарова. - М.: МЦНМО, 2009. - 616 с.:ил.
8. Белов, Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов - М.: Горячая линия- телеком, 2006. - 544 с.

9. Запечников, С. В. Информационная безопасность открытых систем. Том 2. Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков -М.: Горячая Линия -Телеком, 2008. — 560 с
10. Зегжда, Д.П. Основы безопасности информационных систем: учеб. Пособие / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия-телеком, 2000 . - 451 с.
11. Джеймс Питерсон Теория сетей Петри и моделирование систем: Пер. с англ. / Джеймс Питерсон. - М.:Мир, 1984.-264 с, ил.
12. Котенко, И.В. Восстановление формальных грамматик, задающих сценарии компьютерных атак, по прецедентам / И.В. Котенко // "Искусственный интеллект". № 3, 2002. – С.58-67.
13. Барсуков, В.С.Современные технологии безопасности / В.С. Барсуков, В.В. Водолазний. - М.: «Нолидж», 2000. - 496 с.