МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ

ЛІЩИНСЬКИЙ ВЛАДИСЛАВ СЕРГІЙОВИЧ

УДК 004.415

ДОСЛІДЖЕННЯ МЕТОДІВ ІДЕНТИФІКАЦІЇ ЗАГРОЗ В СЕРЕДОВИЩІ БЕЗПРОВІДНИХ МЕРЕЖ

125 «Кібербезпека»

Автореферат
дипломної роботи на здобуття
освітнього рівня «магістр»

Тернопіль
2019

Роботу виконано на кафедрі кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: доктор технічних наук, професор кафедри кібербезпеки
Карпінський Микола Петрович,
Тернопільський національний технічний університет
імені Івана Пулюя,

Рецензент: доктор технічних наук, професор кафедри
комп'ютерних наук
Пасічник Володимир Володимирович,
Тернопільський національний технічний університет
імені Івана Пулюя,

Захист відбудеться 26 грудня 2019 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії №32 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд. 806

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Комп'ютерні системи та телекомунікації забезпечують надійність функціонування великої кількості інформаційних систем різноманітного призначення. Більшість таких систем несуть у собі інформацію конфіденційного характеру. Таким чином, вирішення задачі автоматизації процесів обробки даних спричиняє проблему інформаційної безпеки, при цьому актуальною проблемою є своєчасне виявлення аномальної та/або відхилення від нормальною роботи ПЗ та забезпечення безпеки бездротових мереж.

Однією з істотних проблем при проектуванні та експлуатації систем захисту інформації є нехтування методологією системного аналізу щодо засобів і інструментів для їх захисту. Слід визнати складність, часом неможливість, об'єктивного підтвердження ефективності системи захисту інформації, що багато в чому визначається неповнотою нормативно-методичного забезпечення інформаційної безпеки, перш за все в області показників та критеріїв. Безпека інформації може бути забезпечена лише при комплексному використанні всього набору наявних засобів захисту у всіх структурних елементах виробничої системи на всіх етапах технологічного циклу обробки інформації.

Мета роботи: моделювання процесів ідентифікації кібератак та формалізація принципів побудови класифікатора загроз складових безпеки.

Об'єкт та предмет дослідження. Об'єктом досліджень є загроза в середовищі безпровідних мереж. Предметом дослідження є моделі та алгоритми процесів кібератак, методи захисту інформації.

Наукова новизна отриманих результатів: розширення простору ознак кібератак дає можливість підвищити точність класифікації. Запропонований класифікатор загроз забезпечує можливість формування єдиного підходу щодо визначення загрози та її врахування під час виявлення аномальної роботи, або відхилення від нормальної роботи в середовищі безпровідних мереж на прикладі АБС.

Практичне значення отриманих результатів полягає в тому, що було запропонований класифікатор загроз є універсальним і дозволяє виділити аномалії роботи в будь-якій бездротовій мережі.

Апробація. Окремі результати роботи доповідались на VII науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 11 – 12 грудня 2019 р.

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 7 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 111 арк. формату А4, ілюстративна частина– 18 слайдів.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі сформульовано актуальність проблеми дослідження методів ідентифікації загроз в середовищі безпровідних мереж та сформульовано мету і основні завдання роботи.

У першій главі наведено основні теоретичні відомості щодо тематики роботи.

У другій главі проведено аналіз протоколів забезпечення конфіденційності, цілісності та автентичності даних.

У третій главі наведено методику моделювання процесів кібербезпеки на основі моделі класів кібератак.

В спеціальній частині описано сучасні програми - аналізатори мережевого трафіку.

В п'ятому розділі обчислено основні показники економічної ефективності від розробки і реалізації запропонованого алгоритму.

У підрозділі "Охорона праці" розглянуто правила охорони праці під час експлуатації електронно-обчислювальних машин У підрозділі "Безпека життєдіяльності" описано окремі питання безпеки у виробничих приміщеннях.

В розділі "Екологія" по радіоекології та роботі з банками екологічної інформації.

У загальних висновках щодо дипломної роботи наведено короткий опис основної частини; сформульовано основні результати, отримані в роботі та описано переваги запропонованого класифікатора загроз.

В додатках до пояснювальної записки приведено тези.

В ілюстративній частині приведено Загальна класифікація загроз АБС, Дослідження загроз на протоколи IP-мереж, Класифікація кібератак, Вплив атак на рівнях мережевої моделі OSI, Моделі аналізу ризиків ІБ, Класифікація методів виявлення аномалій та зловживань, Алгоритм класифікатора, Висновки.

ВИСНОВКИ.

Запропонований класифікатор загроз забезпечує можливість формування єдиного підходу щодо визначення загрози та її врахування під час виявлення аномальної роботи, або відхилення від нормальної роботи в середовищі безпровідних мереж на прикладі АБС.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. М. Шмигельський, Основні методи і прийоми порушення безпеки сучасних бездротових мереж [Текст] / М. Шмигельський, В. Ліщинський Збірник тез VII науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» – Тернопіль (11 – 12 грудня 2019 р.), ТНТУ, 2019. – с.106

АНОТАЦІЯ

Дана магістерська кваліфікаційна робота присвячена дослідженню методів ідентифікації загроз в безпровідних мережах. Проведено дослідження засобів і механізмів забезпечення інформаційної безпеки та достовірності інформації в середовищі безпровідних мереж. Для отримання якісної оцінки кібератак і їх подальшої класифікації, запропоновано застосувати відому просторі ознак

класифікацію. Такий підхід дозволив розширити простір ознак для опису невідомих класів кібератак.

Ключові слова: БЕЗПРОВІДНІ МЕРЕЖІ, WI-FI, ОС, ЗАГРОЗИ, РИЗИКИ, АНОМАЛІЇ, SSL, TLS, IPSEC, КЛАСИФІКАТОР ЗАГРОЗ.

ANNOTATION

This master's qualification thesis is devoted to the study of methods of threats identification in wireless networks. Research on the means and mechanisms for ensuring information security and reliability of information in the wireless network environment has been made. In order to obtain a qualitative assessment of cyber attacks and their further classification, it is proposed to apply the known space of classification features. This approach made it possible to extend the space of features to describe unknown classes of cyberattacks.The paper proposes a classifier of threats, which provides the possibility of creating a unified approach to detect the threat when detecting abnormal work, or deviating from normal work in a wireless network environment.

Key words: WIRELESS NETWORKS, WI-FI, OS, THREATS, RISKS, ANOMALIES, SSL, TLS, IPSEC, THREAT CLASSIFIER.