Додаток 1
Форма відомостей про авторів матеріалу та описова інформація для видань ТНТУ

Авторська довідка

(кваліфікаційної роботи магістра)

Назва кваліфікаційної роботи магістра *Створення системи виявлення вторгнень на основі архітектури штучної імунної системи*
назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Creation of an intrusion detection system based on the architecture of an artificial immune system*
переклад англійською

Освітній ступінь : магістр

Шифр та назва спеціальності: 125 «Кібербезпека»
напр.:151 Автоматизація та комп'ютерно-інтегровані технології

Екзаменаційна комісія: Екзаменаційна комісія № 41
напр.: Екзаменаційна комісія №1

Установа захисту: Тернопільський національний технічний університет імені Івана Пулюя
напр.: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 27 грудня 2023 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 77

УДК: 004.056.53:004.77

Автор роботи
Прізвище, ім'я, по батькові (укр.): Черник Олег Андрійович
розкривати ініціали

Прізвище, ім'я (англ.): Chernyk Oleh
використовувати паспортну транслітерацію (КМУ 2010)

Місце навчання (установа, факультет, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра кібербезпеки, м.Тернопіль, Україна

Керівник
Прізвище, ім'я, по батькові (укр.): Баран Ігор Олегович
повністю

Прізвище, ім'я (англ.): Baran Ihor
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Україна

Вчене звання, науковий ступінь, посада: кандидат технічних наук, доцент, декан ФІС

Рецензент
Прізвище, ім'я, по батькові (укр.): Литвиненко Ярослав Володимирович
повністю

Прізвище, ім'я (англ.): Lytvynenko Yaroslav
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра комп'ютерних систем та мереж, м.Тернопіль, Україна

Вчене звання, науковий ступінь, посада: доктор технічних наук, доцент кафедри

Ключові слова
українською: алгоритм клональної селекції, алгоритм негативного відбору, імунні системи розпізнавання, система виявлення вторгнень, формальна імунна система, штучна імунна система
до 10 слів

англійською: clonal selection algorithm, negative selection algorithm, immune recognition systems, intrusion detection system, formal immune system, artificial immune system

до 10 слів

Анотація

українською:

Здійснено критичний огляд мережевих загроз, описані різні мережеві атаки. Виконано аналіз сучасних систем виявлення вторгнень, приведено їх класифікацію за місцем збору інформації, швидкістю реагування та механізмом виявлення. Наведено типову архітектуру системи виявлення вторгнень. Також описано штучні імунні системи, особливості використання алгоритмів клональної селекції і негативного відбору.

Пропонується для детектування аномальних запитів застосувати формальні імунні системи та імунні системи розпізнавання. Два ці підходи інтегруються в складову аналізу системи виявлення вторгнень. При використанні імунокомп'ютингу сформовано алгоритм побудови формальної імунної системи. В основі розробленої системи виявлення вторгнень лежить клієнт-серверна архітектура. Навчання системи виявлення вторгнень та генерація трафіку проходили із використанням набору даних CICIDS 2017.

Проаналізовано ефективність функціонування пропонованої системи виявлення вторгнень. Отримані результати експериментів свідчать, що штучна імунна система може успішно бути застосована для виявлення різних мережевих вторгнень.

англійською:

A critical review of network threats is carried out, various network attacks are described. The analysis of modern intrusion detection systems was performed, and their classification based on the location of information collection, response speed, and detection mechanism was provided. A typical architecture of an intrusion detection system is given. Artificial immune systems, features of using clonal selection algorithms and negative selection are also described.

It is proposed to use formal immune systems and immune recognition systems to detect abnormal requests. These two approaches are integrated into the analysis component of the intrusion detection system. When using immunocomputing, an algorithm for building a formal immune system was formed. The basis of the developed intrusion detection system is the client-server architecture. The intrusion detection system was trained and traffic generated using the CICIDS 2017 dataset.

The effectiveness of the proposed intrusion detection system was analyzed. The experimental results show that the artificial immune system can be successfully applied to detect various network intrusions.

Бібліографічний опис:

Черник О. А. Створення системи виявлення вторгнень на основі архітектури штучної імунної системи: кваліфікаційна робота магістра за спеціальністю 125 — Кібербезпека / Черник Олег Андрійович – Тернопіль : ТНТУ, 2023. – 77 с.

Chernyk O. Creation of an intrusion detection system based on the architecture of an artificial immune system: Master thesis 125 — Cybersecurity / Chernyk Oleh - Ternopil, TNTU, 2023 – 77 p.