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

Авторська довідка
(кваліфікаційної роботи магістра)

Назва кваліфікаційної роботи магістра: Можливості застосування штучного інтелекту в Операційному центрі безпеки

Назва (англ.): : Possibilites of artificial intelligence application in the security operations center

Освітній ступінь : магістр

Шифр та назва спеціальності: 125 Кібербезпека

Екзаменаційна комісія: Екзаменаційна комісія № 41

Установа захисту: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 26 грудня 2023 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 85

УДК: 004.056

Автор роботи
Прізвище, ім'я, по батькові (укр.): Задорожний Святослав Юрійович

Прізвище, ім'я (англ.): Zadorozhnyi Sviatoslav

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.): Скарга-Бандурова Інна Сергіївна

Прізвище, ім'я (англ.): Skarga-Bandurova Inna

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

Вчене звання, науковий ступінь, посада: д.т.н., проф., професор кафедри кібербезпеки

Рецензент
Прізвище, ім'я, по батькові (укр.): Боднарчук Ігор Орестович

Прізвище, ім'я (англ.): Bodnarchuk Ihor

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

Вчене звання, науковий ступінь, посада к.т.н., доцент, завідувач кафедри КН

Ключові слова
українською: центр операцій з безпеки, інформаційна безпека, комплекс засобів захисту, штучний інтелект, машинне навчання

англійською: security operation center, information security, protection suite, artificial intelligence, machine learning

Анотація
українською: Основна мета цього дослідження полягає у вдосконаленні систем запобігання інтрузій (IPS), систем управління інформаційною безпекою (SIEM) та систем запобігання витоку даних (DLP) у контексті центрів операцій з безпеки (SOC) за допомогою методів штучного інтелекту (ШІ) та машинного навчання (МН). Дослідження спрямоване на виявлення та аналіз проблем та викликів, що виникають у зазначених системах, та визначення можливостей їх подолання за допомогою передових технологій.
В рамках кваліфікаційної роботи проаналізовано концепції і підходи організації центрів операційної безпеки на базі ШІ. Також виконано порівняння різних підходів до побудови SOC центру, визначені переваги і недоліки цих концепцій. Запропонована метрика і підходи до оцінювання системи побудованної на принципах уніфікації та поєднання ШІ.

англійською: The main goal of this research is to improve Intrusion Prevention Systems (IPS), Security Information and Event Management (SIEM) systems, and Data Loss Prevention (DLP) systems in the context of Security Operations Centers (SOC) using Artificial Intelligence (AI) and Machine Learning (ML) methods. The research aims to identify and analyze problems and challenges in the mentioned systems and determine the possibilities of overcoming them using advanced technologies.
Within the scope of the qualification thesis, concepts and approaches to the organization of security operations centers based on AI are analyzed. A comparison of different approaches to building SOC centers is also performed, identifying the advantages and disadvantages of these concepts. A metric and approaches to evaluating a system built on the principles of unification and the combination of AI are proposed.

Бібліографічний опис:
Задорожний С. Ю. Можливості застосування штучного інтелекту в операційному центрі безпеки: кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю „125 — кібербезпека“ / С. Ю. Задорожний. — Тернопіль: ТНТУ, 2023. — 85 с.