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

Авторська довідка

(кваліфікаційної роботи бакалавра)

Назва кваліфікаційної роботи бакалавра Створення автоматизованої системи аналізу журналів для виявлення аномалій і загроз безпеки в комп'ютерній системі
назви записувати нижнім регістром (як у реченні)

Назва (англ.): Creation of an automated log analysis system for detecting anomalies and security threats in a computer system
переклад англійською

Освітній ступінь : бакалавр

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

Екзаменаційна комісія: Екзаменаційна комісія № 40
напр.: Екзаменаційна комісія №1

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

Дата захисту: 20 червня 2023 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 51

УДК: 004.056

Автор роботи
Прізвище, ім'я, по батькові (укр.): Микитюк Тарас Володимирович
розкривати ініціали

Прізвище, ім'я (англ.): Mykytiuk Taras
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.): Козак Руслан Орестович
повністю

Прізвище, ім'я (англ.): Kozak Ruslan
використовувати паспортну транслітерацію (КМУ 2010)

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

Вчене звання, науковий ступінь, посада: кандидат технічних наук

Рецензент
Прізвище, ім'я, по батькові (укр.): Михалик Дмитро Михайлович
повністю

Прізвище, ім'я (англ.): Mykhalyk Dmytro
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 наук, м.Тернопіль, Україна

Вчене звання, науковий ступінь, посада: к.т.н., доцент кафедри ПІ

Ключові слова
українською: автоматизація, аналіз, виявлення аномальної поведінки.
до 10 слів

англійською: automation, analysis, detection of abnormal behavior.
до 10 слів

Анотація
українською:

Кваліфікаційна робота присвячена розробці системи виявлення аномалій поведінки користувачів для виявлення вразливостей, атак та інших загроз безпеки комп'ютерної системи. Розроблена система допоможе забезпечити безпеку комп'ютерної системи та підвищить ефективність процесу виявлення вразливостей та реагування на можливі загрози.

У першому розділі кваліфікаційної роботи було розглянуто функції систем виявлення і запобігання вторгнень а також SIEM, види журналів та методи аналізу журналів подій.

У другому розділі було розглянуто питання автоматизції аналізу журналів подій, а також визначено критерії виявлення аномалій і загроз безпеки.

У третьому розділі було розроблено і протестовано систему автоматичного аналізу журналів подій.

англійською:

The qualification work is devoted to the development of a system for detecting anomalies in user behavior to detect vulnerabilities, attacks and other threats to the security of the computer system. The developed system will help to ensure the security of the computer system and increase the efficiency of the process of detecting vulnerabilities and responding to possible threats.

In first section of the qualification work, the functions of intrusion detection and prevention systems, as well as SIEM, types of logs and methods of analyzing event logs were considered.

In the second section, the issue of automating the analysis of event logs was considered, as well as the criteria for detecting anomalies and security threats were defined.

In the third section, a system for automatic analysis of event logs was developed and tested.

.

Бібліографічний опис:

Микитюк Т.В. Створення автоматизованої системи аналізу журналів для виявлення аномалій і загроз безпеки в комп'ютерній системі: кваліфікаційна робота бакалавра за спеціальністю 125 — Кібербезпека / Т.В. Микитюк. – Тернопіль : ТНТУ, 2023. – 51 с.