**Додаток 1**

Форма відомостей про авторів матеріалу та описова інформація для видань ТНТУ

**Авторська довідка**

*(кваліфікаційної роботи бакалавра)*

**Назва кваліфікаційної роботи бакалавра** Методи та засоби аналізу журналів подій Sophos Firewall

*назви записувати нижнім регістром (як у реченні)*

**Назва (англ.):** Methods and tools for analyzing event logs from Sophos Firewalls

*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:** 21 червня 2023 року  **Місто:** Тернопіль

**Сторінки:**

Кількість сторінок роботи: 61

**УДК:**

**Автор роботи**

Прізвище, ім’я, по батькові (укр.): Пилипів Павло Вололодимирович

розкривати ініціали

Прізвище, ім’я (англ.): Pylypiv Pavlo

*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.): Лечаченко Тарас Анатолійович

повністю

Прізвище, ім’я (англ.): Lechachenko Taras

*використовувати паспортну транслітерацію (КМУ 2010)*

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

Вчене звання, науковий ступінь, посада: д.філ., асистент кафедри кібербезпеки

**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

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

**Ключові слова**

українською: аналіз, журнали подій, логи, міжмережеві екрани, Sophos Firewall XG. *до 10 слів*

англійською: analysis, event logs, logs, firewalls, Sophos Firewall XG.

*до 10 слів*

**Анотація**

українською:

Кваліфікаційна робота присвячена створенню алгоритму аналізу журналів подій у вигляді конфігураційного файлу, який проводить аналіз та структуризацію інформації з журналів подій.

У першому розділі кваліфікаційної роботи описані можливості міжмережевого екрану нового покоління Sophos Firewall XG, проаналізовано публікації, які стосуються об’єкту дослідження, обрано та обґрунтовано методи отримання та аналізу журналів подій.

У другому розділі кваліфікаційної роботи розглянуті етапи аналізу подій в ІКС, механізми збору, опрацювання та збереження журналів подій. Проаналізовані методи логування.

У третьому розділі кваліфікаційної роботи описано розгортання програмного забезпечення для аналізу, зберігання та візуалізації журналів подій. Створено конфігураційний файл який проводить аналіз та структуризацію інформації з журналів подій. Візуалізовано отримані дані в інформаційній панелі з допомогою Kibana.

англійською:

The qualification work is devoted to the creation of an algorithm for analyzing event logs in the form of a configuration file, which analyzes and structures information from event logs.

The first section of the qualification work describes the capabilities of the next generation firewall Sophos Firewall XG, analyzes the publications related to the researched object, selects and substantiates the methods of obtaining and analyzing event logs.

In the second section of the qualification work, considered the stages of event analysis in ICS, mechanisms for collecting, processing and saving event logs. Analyzed logging methods.

The third chapter of the qualification paper describes the deployment of software for analysis, storage and visualization of event logs. A configuration file has been created that analyzes and structures information from event logs. The received data was visualized in the information panel using Kibana.

Бібліографічний опис:

Пилипів П. В. Методи та засоби аналізу журналів подій Sophos firewall: кваліфікаційна робота бакалавра за спеціальністю 125 — Кібербезпека / П. В. Пилипів. – Тернопіль : ТНТУ, 2023. – 62 c.