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

Авторська довідка

(кваліфікаційної роботи магістра)

Назва кваліфікаційної роботи магістра Розробка системи безпеки для IoT з використанням SIEM технологій
назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Development of security system for IoT using SIEM technologies*
переклад англійською

Освітній ступінь : магістр

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

Екзаменаційна комісія: Екзаменаційна комісія № 47
напр.: Екзаменаційна комісія №1

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

Дата захисту: 21 грудня 2022 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 54

УДК: 004.056

Автор роботи
Прізвище, ім'я, по батькові (укр.): Маслій Ростислав Богданович
розкривати ініціали

Прізвище, ім'я (англ.): Maslii Rostislav
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.): Скарга-Бандурова Інна Сергіївна
повністю

Прізвище, ім'я (англ.): Skarha-Bandurova Inna
використовувати паспортну транслітерацію (КМУ 2010)

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

Вчене звання, науковий ступінь, посада: професор

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: доцент кафедри КН

Ключові слова

СИСТЕМА БЕЗПЕКИ, МЕРЕЖА ІНТЕРНЕТУ РЕЧЕЙ, SIEM, IOT, ТЕХНОЛОГІЯ

до 10 слів

SECURITY SYSTEM, INTERNET OF THINGS NETWORK, SIEM, IOT, TECHNOLOGY

до 10 слів

Анотація

Метою роботи є дослідження технологій управління інформаційною безпекою та розробка системи безпеки для IoT на підставі SIEM технології. Основні результати роботи: досліджено площу діяльності новітніх IoT пристроїв та їх передачу даних через проколи, що в свою чергу дозволило краще визначити переваги та недоліки для розробки власної системи. Проаналізовано декілька технологій управління інформаційної безпекою, серед доступних на ринку. Аналіз проводився в першу чергу, для того, щоб обрати підходящу систему для конкретних пристроїв та обслуговування системи було дешевим і водночас якісним порівняно з конкурентами. На підставі проведеного досліження створено безпеки для IoT за допомогою Elastic Stack SIEM. У першому розділі описується сучасний стан безпеки IoT систем, а також технологій зв'язку, протоколів передачі даних та архітектуру IoT систем. У другому розділі проаналізовано найбільш актуальні SIEM системи, описано їхні недоліки та переваги.
Третій розділ – практична частина. У ньому описано деталі розробки системи безпеки пристроїв мережі Інтернет речей. Система здатна самостійно аналізувати та сповіщати користувача про події, які можуть загрожувати безпеці. Завдяки цьому моніторингу, можливо швидко реагувати на інциденти та побачити їх у вигляді візуалізації на панелі адміністратора мереж. У четвертому розділі описано інструкції з охорони праці при роботі з комп'ютером та фактори виробничого середовища і їх вплив на життєдіяльність людини.
В розділі " Безпека в надзвичайних ситуаціях " описано питання здоров'я працівників,додано поради щодо його покращення та як воно впливає на професійну діяльність.

The purpose of the work is to study information security management technologies and develop a security system for IoT based on SIEM technology. The main results of the work: the area of activity of the latest IoT devices and their data transmission through the punctures were investigated, which in turn allowed to better determine the advantages and disadvantages for the development of their own system. Several information security management technologies available on the market were analyzed. The analysis was carried out primarily in order to choose a suitable system for specific devices and to ensure that the system maintenance was cheap and at the same time of high quality compared to competitors. Based on the conducted research, security for IoT using Elastic Stack SIEM was created. The first section describes the current state of security of IoT systems, as well as communication technologies, data transfer protocols and architecture of IoT systems.The second section analyzes the most relevant SIEM systems, describes theirdisadvantages and advantages.The third section is a practical part. It describes the details of developing a security system for Internet of Things devices. The system is able to independently analyze and notify the user about events that may threaten security. Thanks to this monitoring, it is possible to quickly respond to incidents and see them in the form of visualization on the network administrator panel. The fourth section describes occupational safety instructions when working with computers and factors of the production environment and their impact onhuman life. The section "Safety in Emergency Situations" describes the health of employees, adds tips for its improvement and how it affects professional activities.