МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ «АСТАНА»

ІНФОРМАТИКА, МАТЕМАТИКА, АВТОМАТИКА

ІМА - 2023

МАТЕРІАЛИ
та програма

МІЖНАРОДНОЇ
НАУКОВОЇ КОНФЕРЕНЦІЇ
молодих учених

(Суми-Астана,
24-28 квітня 2023 року)

Суми,
Сумський державний університет
2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ «АСТАНА»

ІНФОРМАТИКА, МАТЕМАТИКА, АВТОМАТИКА

IMA :: 2023

МАТЕРІАЛИ
та програма

МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ
молодих учених

(Суми – Астана, 24–28 квітня 2023 року)

Суми
Сумський державний університет
2023

СЕКЦІЯ № 1 «КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА»

Голова секції – д-р. тех. наук, проф. Довбиш А.С.
Секретар секції – провідний фахівець Лук'яніхіна А.Ф.

Початок: 26 квітня 2023 р., онлайн, 13^{00}
https://us02web.zoom.us/j/5085263824?pwd=VHI1RjNKUG9TY3hLeFRTUERtYko0UT09

1. Enhanced EIGRP Application in Software-Defined Networking

   Authors: Stud. Horiainova K.,
   Stud. Kapusta R.
   Supervisor – Prof. Yeremenko O.

2. Enhancing the Security of Critical Infrastructure Powered by SCADA

   Author – PhD Stud. Joel Kashaija

3. Development of a Threat Model when Ensuring Information Security in Messengers Based on Privacy and Anonymity

   Author – Stud. Maiba M.
   Supervisor – Prof. Yeremenko O.

4. End-to-End Network Resilience, Security, and QoS in SD-WAN

   Authors: Stud. Nedostup D.,
   Stud. Solomianyi M.,
   Stud. Mamon R.
   Supervisor – Prof. Yeremenko O.

5. Comparison of Network Configuration Management Tools

   Authors: Stud Persikov M.,
   Stud. Lemeshko V.,

Stud. Khikhlo V.
Supervisor – Prof. Yeremenko O.

6. Роль інтернет-технологій в бізнесі

   Автори: здобувач Гец Д.О.,
   здобувач Сазанова А.А.,
   доц. Нефедченко В.Ф.,
   ст. викл. Коваль В.В.

7. Створення програмного додатку для навігаційної системи

   Автори: здобувач Боднар С.Д.,
   здобувач Герасимюк І.Р.,
   доц. Маслова З.І.

8. Трафік в мережах: перехоплення та аналіз

   Автори: здобувач Підлісна А.А.,
   ст. викл. Кальченко В.В.,
   ст. викл. Коваль В.В.

9. Нейромережеве вимірювання рівня води в трубопроводі водовідведення за даними відеоінспекції

   Автор – викладач-стажист Зарецький М.О.

10. Інформаційна технологія інтелектуального аналізу даних відеоінспекції трубопроводу водовідведення

    Автор – викладач-стажист Зарецький М.О.

11. Використання фреймворків

    Автори: здобувач Войтенко Д.Р.,
    доц. Нефедченко В.Ф.,

СЕКЦІЯ 1

«Комп’ютерні науки та кібербезпека»

Enhancing the Security of Critical Infrastructure Powered by SCADA

Joel Kashaija, *PhD student*

Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Building cyber resilience for critical infrastructure (CI) running on SCADA is a complex and multifaceted process that requires careful planning, deployment, and maintenance. The threat landscape has evolved significantly recently, with cyber-attacks becoming more frequent, sophisticated, and damaging. Organizations must take a holistic approach encompassing various measures to protect SCADA systems from these threats effectively. A typical SCADA system contains the following features.

Identifying and evaluating possible threats is one of the crucial components in constructing cyber resilience for CI. This entails conducting a thorough risk analysis considering all potential attack vectors, including internal and external threats. Organizations can create and deploy various security measures to reduce threats after they have been recognized.

Creating a secure network design is pivotal to enhancing cyber resilience for CI. SCADA networks must be separated from other corporate networks to prevent unwanted access, and strict access restrictions must be implemented. By reducing the attacker's capacity to move laterally across the network, its segmentation can considerably lower the chance of a successful cyber assault.

Establishing incident response plans is also critical to building cyber resilience for CI. These plans should outline the steps during a security breach, including who to notify, how to contain the incident, and how to restore systems to regular operation.

Finally, ongoing maintenance and updates are essential to ensuring the continued effectiveness of cyber resilience measures. This includes regularly updating software and firmware, applying security patches, and conducting regular audits to ensure compliance with security policies and standards.

Building cyber resilience for critical infrastructure running on SCADA requires a comprehensive and continuous effort involving multiple organizational stakeholders. By implementing various measures that address both technical and non-technical aspects of cybersecurity, organizations can significantly reduce the risk of a successful cyber attack and protect their critical infrastructure from harm.