Науково-дослідна частина
Національного університету
кораблебудування
імені адмірала Макарова

54025, м. Миколаїв,
пр. Героїв України, 9
Тел.: (0512) 70-91-04
http://conference.nuos.edu.ua
e-mail: conference@nuos.edu.ua

Навчально-науковий інститут
автоматики та електротехніки
Національного університету
кораблебудування
імені адмірала Макарова

54021, м. Миколаїв,
пр. Центральний, 3
Тел.: (0512) 47-70-95
http://iae.nuos.edu.ua
e-mail: university@nuos.edu.ua

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

НАУКОВО-ТЕХНІЧНІ КОНФЕРЕНЦІЇ
Національний університет кораблебудування
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

МАТЕРІАЛИ

XI ВСЕУКРАЇНСЬКОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ

23-24 листопада 2023 р.

Миколаїв ■ НУК ■ 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2023

МАТЕРІАЛИ

XI Всеукраїнської науково-технічної конференції з міжнародною участю

23–24 листопада 2023 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МИКОЛАЇВ • НУК • 2023

УДК 004
У 45

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»

Матеріали публікуються за оригіналами, наданими авторами.
Претензії до організаторів не приймаються.

Відповідальна за випуск В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв : НУК, 2023. – 223 с.

У збірнику подано матеріали XI Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, системи Інтернет речей (IoT), моделювання об'єктів і процесів технічного захисту інформації, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

УДК 004.056.5:004.738.5

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ВІДДАЛЕНОМУ КЕРУВАННІ ЛАБОРАТОРНИМ ОБЛАДНАННЯМ СТЕНДУ «ЦИФРОВИЙ АВТОМАТ»

Автор: *Клєошин С.К., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Трибулькевич С.Л., ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Метою роботи є дослідження проблем інформаційної безпеки, які виникають при віддаленому керуванні лабораторним обладнанням стенду “Цифровий автомат” та аналіз загроз, пов’язаних з цим видом роботи, а також розробка заходів для їх уникнення.

У сучасному світі швидкість змін та технологічних розробок безперервно зростає, що ставить перед науково-дослідними та навчальними установами нові виклики щодо ефективного використання лабораторного обладнання. Одним із відповідей на ці виклики стало впровадження систем віддаленого керування лабораторним обладнанням.

Віддалене керування лабораторним обладнанням відкриває широкі можливості для досліджень, навчання та інженерних проектів, дозволяючи використовувати дорогоцінне обладнання з будь-якого місця, де є доступ до Інтернету. Це особливо важливо в умовах сучасної пандемії, коли віддалена робота та навчання стали необхідністю.

Однак разом з безсумнівними перевагами віддаленого керування приходять і нові виклики, зокрема у сфері інформаційної безпеки. Забезпечення захисту систем віддаленого доступу до лабораторного обладнання стає пріоритетним завданням для забезпечення конфіденційності, цілісності та доступності даних.

У цьому контексті вивчення проблем інформаційної безпеки при віддаленому керуванні лабораторним обладнанням набуває особливого значення, адже воно спрямоване на розуміння потенційних загроз та розробку ефективних стратегій захисту, що дозволить максимально використовувати переваги віддаленого доступу без ризику порушення безпеки.

Проблеми інформаційної безпеки при віддаленому керуванні лабораторним обладнанням можуть включати:

– Несанкціонований доступ: ризик отримання несанкціонованого доступу до системи через віддалене підключення. Це може призвести до втрати конфіденційної інформації або навіть зміни параметрів обладнання.

– Збій зв'язку: віддалене керування вимагає стабільного зв'язку між користувачем і обладнанням. Відсутність зв'язку може призвести до неправильної роботи або навіть аварії.

– Конфіденційність даних: передача даних через мережу може бути підвергнута ризику перехоплення або несанкціонованого доступу. Важливо забезпечити шифрування та захист даних.

– Цілісність даних: ризик зміни даних під час передачі або керування. Заходи повинні бути вжиті для запобігання незаконним змінам.

З історії інтернету виокремлюються декілька видатних хакерських атак на системи автоматики та інформаційні системи:

– Взлом Міжнародної космічної станції (МКС): У 1999 році 15-річний хакер Джонатан Джеймс взламав сервери NASA, отримавши доступ до системи життєзабезпечення МКС. Це був серйозний інцидент, який вимагав посилення заходів безпеки.

– **Вірус Stuxnet**, виявлений у 2010 році, спрямований на іранську ядерну програму. Він вразив системи керування промисловими процесами, такими як центрифуги для збагачення урану.

– Ukraine Power Grid Attack (2015-2016). Ця атака сталася в грудні 2015 та січні 2016 року і призвела до вимкнення електроенергії в певних районах України. Хакери використовували шкідливе програмне забезпечення, щоб перехопити системи керування енергомережею та заблокувати їх роботу.

– Triton / Trisis: Ця атака була виявлена в 2017 році і спрямована на системи керування виробничою безпекою. Хакери використовували шкідливе програмне забезпечення, щоб змінити програмне забезпечення контролерів безпеки, що призвело до небезпеки для робітників та можливого аварійного виробництва.

– Dragonfly (Havex): Ця атака, також відома як Energetic Bear, спрямована на системи керування електромережею та інші промислові системи в окремих країнах. Хакери використовували різні методи,

включаючи фішинг та використання вразливостей програмного забезпечення, щоб отримати доступ до систем керування та спостереження.

Керування обладнанням через глобальну мережу вимагає використання різних методів та засобів для забезпечення безпеки та ефективності, таких як забезпечення безпечних тунелів між віддаленими пристроями через глобальну мережу, шифрування та аутентифікація (використання SSL/TLS для шифрування даних під час передачі, встановлення паролів, двофакторної аутентифікації та інших методів для захисту доступу).

Вирішення проблем інформаційної безпеки при віддаленому керуванні лабораторним обладнанням стенду "Цифровий Автомат" вимагає комплексного підходу та застосування різноманітних заходів забезпечення безпеки:

1. Захист мережі: забезпечення безпеки мережі за допомогою захисту мережевого периметру, використання файрволів, інтранетів, VPN тунелів та інших засобів.

2. Сильні паролі та аутентифікація: від користувачів вимагається використання складних паролів, двофакторної аутентифікації та регулярної зміни паролів.

3. Шифрування даних для захисту передаваних даних через мережу, особливо у випадку чутливої інформації.

4. Моніторинг та журналювання для виявлення незвичайних активностей або спроб несанкціонованого доступу.

5. Обмеження доступу: доступ до лабораторного обладнання надається лише авторизованим користувачам та обмежуються їхні права доступу згідно з принципом найменших привілеїв.

6. Захист від вірусів та шкідливих програм: використання антивірусного програмного забезпечення та інші заходи захисту від шкідливих програм.

7. Планування кризових ситуацій: розроблення плану дій у випадку порушення безпеки, який включає в себе процедури реагування та відновлення після інциденту.

8. Навчання користувачів: проведення навчання з питань інформаційної безпеки для користувачів, щоб вони були усвідомлені та вміли виявляти можливі загрози.

9. Аудит безпеки для оцінки ефективності заходів безпеки та виявлення нових загроз.

Висновки. Забезпечення безпеки при віддаленому доступі до лабораторних систем є надзвичайно важливим завданням. Підвищення популярності віддалених робочих середовищ, супроводжується зростанням ризиків та загроз інформаційній безпеці.

У результаті дослідження встановлено, що ключовими проблемами безпеки при віддаленому керуванні є незахищені мережеві підключення, вразливість систем та відсутність ефективних механізмів аутентифікації та авторизації. Для ефективного рішення цих проблем рекомендується впровадження комплексу заходів, таких як захист мережі, сильні паролі та аутентифікація, шифрування даних, регулярні оновлення, моніторинг та журналювання, обмеження доступу, захист від вірусів та шкідливих програм, планування кризових ситуацій, освіта та навчання користувачів та аудит безпеки.

Враховуючи ці рекомендації, можна значно підвищити рівень інформаційної безпеки при віддаленому керуванні лабораторним обладнанням стенду "Цифровий Автомат", що дозволить зменшити ризики зловживання та зберегти конфіденційність, цілісність та доступність даних.

Список літератури:

1. Клік, М. (2017). "Кібербезпека виробничих систем керування: загрози та заходи захисту". Комп'ютерні науки та інформаційні технології, 4, 22-31.

2. Петренко, О., & Сімонов, В. (2018). "Кібератаки на індустріальні системи керування: аналіз та захист". Інформаційно-керуючі системи на залізничному транспорті, 2(26), 101-109.

3. Кравченко, О., & Шевчук, В. (2019). "Захист від кібератак на системи автоматизації виробничих процесів". Інформаційні технології та комп'ютерна інженерія, 3(69), 81-88.

4. Гріньов, Д. (2020). "Кібербезпека в індустріальних системах керування: актуальні проблеми та заходи захисту". Інженерія безпеки, 2(43), 42-48.

5. Барановський, О., & Гончаренко, С. (2016). "Загрози та заходи захисту від кібератак на системи автоматизації промислових підприємств". Інформаційні технології та комп'ютерна інженерія, 1(63), 106-113.

6. Stouffer, K., Falco, J., & Scarfone, K. (2011). "Guide to Industrial Control Systems (ICS) Security". NIST Special Publication 800-82.

7. Langner, R. (2011). "Stuxnet: Dissecting a Cyberwarfare Weapon". IEEE Security & Privacy, 9(3), 49-51.

8. Klick, M. (2017). "Cybersecurity Threats to Manufacturing Control Systems - An Overview". IEEE Xplore.

9. Slay, J., & Higgins, G. (2016). "The Cyber Security of Industrial Control Systems - What Does It Mean?" International Journal of Critical Infrastructure Protection, 14, 53-75.

10. Lodi, G., & Zanero, S. (2016). "An Empirical Study of the Reliability of Windows Filtering Platform for the Detection of SCADA-specific Network Traffic". Computers & Security, 62, 78-91.

11. Lee, J., & Kim, H. (2015). "Advanced Persistent Threats and Zero-day Attacks in Industrial Control Systems". International Journal of Control, Automation and Systems, 13(2), 295-302.

12. Bianco, M., Frigieri, F., & Oliva, A. (2017). "Industrial Control System Cyber-Physical Security: A Taxonomy". IFAC-PapersOnLine, 50(1), 4810-4817.

13. Hansman, J., Paulraj, A., & Saberi, S. (2015). "Cyber Physical System Security for Industrial Control Systems". Proceedings of the IEEE, 103(5), 835-848.

14. Luiijf, H., & Chotinaiwattarakul, W. (2013). "Cyber Security in the Energy Sector: Why It's Crucial & How to Improve It". Journal of Critical Infrastructure Policy, 1(1), 97-109.

15. Perrow, C. (2007). "The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters". Princeton University Press.