Міністерство освіти і науки України
Кам’янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет
Кафедра комп’ютерних наук

Дипломна робота
магістра

з теми: **«РОЗРОБКА МЕТОДУ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ В АСУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»**

Виконав: студент групи KN1-M22
спеціальності 122 Комп’ютерні науки
Богуш Дмитро Васильович

Керівник:
Моцик Р. В., доцент кафедри
комп’ютерних наук

Рецензент:
Оптасюк С. В., кандидат фізико-математичних наук, доцент,
доцент кафедри фізики

Кам’янець-Подільський – 2023

ЗМІСТ

ВСТУП

У сучасному світі інтенсивний розвиток технологій супроводжується розширенням та ускладненням критичних інфраструктур, таких як електроенергетика, транспорт, водопостачання та інші, що стає об'єктом зростаючої уваги у галузі кібербезпеки. Автоматизовані системи управління виявляються серцевиною цих інфраструктур та дозволяють ефективно контролювати та управляти великими мережами.

Кіберзагрози та атаки на інформаційні системи критичних інфраструктур стають все більш складними та вдосконаленими, загрожуючи не лише ефективності роботи, але й безпеці та стійкості цих систем. Тому проблема забезпечення кібербезпеки автоматизованих систем управління критичною інфраструктурою стає вельми актуальною.

Актуальність. Актуальність захисту інформації в автоматизованих системах управління критичної інфраструктури визначається різноманітними факторами, які включають в себе технологічний прогрес, зростання кількості кіберзагроз та залежність від інформаційних технологій.

У сучасному світі, де системи управління виробництвом, енергетичні мережі, транспортні системи та інші аспекти критичної інфраструктури стають все більш автоматизованими та підключеними до мережі, захист інформації стає вирішальною складовою стійкості та безпеки цих систем.

Зростання кількості кіберзагроз, таких як атаки вірусами, фішинг, атаки на вторгнення та інші, викликає необхідність постійного удосконалення заходів кібербезпеки. Враховуючи потенційні наслідки кібератак на критичну інфраструктуру, включаючи можливість втрати контролю над системами та порушення нормального функціонування, захист інформації стає завданням вищого пріоритету.

Крім того, розвиток мережі Інтернет та збільшення кількості підключених пристроїв у критичних системах підвищує ризики з точки зору безпеки. Тому актуальність захисту інформації в АСУ критичної інфраструктури не тільки

залишається важливою, але й постійно зростає в умовах швидкого технологічного розвитку та зміни кіберзагроз..

Тема роботи. Розробка методу забезпечення конфіденційності інформації в АСУ критичної інфраструктури.

Мета роботи. Для досягнення успішного результату із виконання магістерської роботи потрібно:

- проаналізувати сучасні рішення щодо забезпечення конфіденційності АСУ КІ;

- вивчення вразливостей, пов’язаних з людським фактором та технічними аспектами;

- вдосконалення функціоналу систем управління для забезпечення ефективного використання ресурсів;

- розробка та впровадження заходів забезпечення конфіденційності інформації в АСУ.

Предметом дослідження захисту інформації є процес розробки інформаційної складової згідно сучасних тенденцій кібербезпеки.

Об’єктом дослідження методу є системи захисту, передачі та обробки інформації.

У процесі дослідження будуть розглянуті такі ключові аспекти, як розробка сучасних методів виявлення та ідентифікації атак, аналіз вразливостей систем, вдосконалення процесів реагування на інциденти та підвищення освідомленності персоналу.

Практичним значенням даної магістерської кваліфікаційної роботи є надійний захист інформації в автоматизованих системах управління критичної інфраструктури.

Задачами проєкту є аналіз тенденцій на ринку програмних застосунків, які забезпечують захист даних, їх збереження, передачу та обробку, необхідного програмного забезпечення, реалізація власного або покращеного уже існуючого методу для надійного захисту інформації.

Структура роботи. Магістерська робота складається із вступу, двох розділів (1 теоретичного і 1 практичного), висновків, 14 рисунків, списку використаних джерел, обсяг роботи становить 53 сторінок.

ВИСНОВОК

В магістерській роботі, присвяченій розробці методу забезпечення конфіденційності інформації в автоматизованих системах управління критичної інфраструктури, виявлено та проаналізовано ключові аспекти кібербезпеки, зокрема в контексті важливості надійного функціонування систем, що керують критично важливими процесами.

Однією з ключових висновків роботи є те, що захист інформації в АСУ критичної інфраструктури є завданням високої важливості в умовах зростаючих кіберзагроз. Аналіз сучасних технічних та організаційних рішень вказує на необхідність комплексного підходу, що охоплює технічні заходи, політики безпеки, моніторинг та освіту персоналу.

Також виявлено, що вибір ефективних технічних засобів для виявлення та захисту від кіберзагроз, таких як системи виявлення вторгнень та засоби шифрування, має велике значення для забезпечення цілісності, конфіденційності та доступності інформації.

У роботі також враховано важливість взаємодії з організаційними структурами, нормативними вимогами та стандартами безпеки для підвищення рівня відповідності та готовності до вирішення можливих інцидентів.

Для реалізації нового методу щодо виявлення та протидії несанкціонованого доступу до АСУ було використано програмний застосунок Snort.

Snort використовує гнучкі правила для виявлення аномальної активності в мережі, дозволяючи аналізувати пакети на предмет підозрілих патернів та сигнатур. Це робить його ефективним інструментом для виявлення різноманітних кіберзагроз, включаючи атаки на вторгнення, атаки на викидання, та інші.

Також, можемо підкреслити гнучкість Snort у налаштуванні та розширенні, що дозволяє адаптувати його під конкретні потреби мережі та забезпечує можливість інтеграції з іншими системами безпеки.

Зазначимо, що, не дивлячись на свою ефективність, Snort має свої обмеження та вимоги, які слід враховувати при його використанні. Потрібно розглядати його як один із компонентів більшої стратегії кібербезпеки, і узгоджувати його роботу з іншими інструментами та заходами захисту, що й було виконано у ході налаштування його роботи і захисту АСУ в цілому.

В ході виконання кваліфікаційної роботи було проаналізовані сучасні рішення щодо забезпечення конфіденційності інформації в автоматизованих системах управління, досліджені потенційних загроз для АСУ критичної інфраструктури, за допомогою наявних методів було розроблено метод для відслідковування та протидії щодо втручання в АСУ, що надало змогу забезпечити конфіденційність та надійне зберігання інформації. В ході роботи було залучено кілька методів відслідковування потенційних загроз і спроб несанкціонованого втручання в систему.

Загалом, дана магістерська робота спрямована на вдосконалення розуміння та реалізацію заходів кібербезпеки в АСУ критичної інфраструктури, надаючи важливий внесок у сферу безпеки в цьому важливому контексті.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Промислові мережі та інтеграційні технології в автоматизованих системах: [навч. посіб.] / Пупена О.М. [та ін.] К. : Вид-во «Ліра-К», 2011. 552 с.

2. Правила для безпеки інформаційних систем та мереж: До культури безпеки 2016. [Електронний ресурс] – Режим доступу до ресурсу: http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD guidelines.pdf.

3. Schjolberg S., Ghernaouti-Hlie S. Глобальний договір про кібербезпеку та кіберзлочинство, Друге видання. [Електронний ресурс] – Режим доступу до ресурсу: http://www.cybercrimelaw.net/documents/.

4. Автоматизація виробничих процесів: Підручник / І.В. Ельперін, О.М. Пупена, В.М. Сідлецький, С.М. Швед . К.: Ліра-К, 2015. 378 с.

5. Організація комп’ютерних мереж: Підручник / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Київ: КПІ ім. Ігоря Сікорського, 2018. 259с.

6. Лукінюк М.В. Автоматизація типових технологічних процесів: технологічні об’єкти керування та схеми автоматизації: Навчальний посібник. – К.: НТУУ “КПІ”, 2008. 236 с.

7. Денисенко В.В. Комп'ютерне управління технологічним процесом, експериментом, обладнанням. М .: Гаряча лінія-Телеком, 2009. 608 с.

8. Автоматизовані системи керування технологічними процесами: Підручник / За редакцією І.О. Фурмана. Харків: Факт, 2006. 317 с.

9. Ігнатьєв А. А. Удосконалення управління якістю продукції на основі системи моніторінга з елементами штучного інтелекту / А. А. Ігнатьєв, Є. М. Самойлова // Вісник СГТУ. 2009. № 3(41). С. 207–209.

10. Островерхов М.Я., Сільвестров А. М., Скриннік О.М. Системи і методи ідентифікації електротехнічних об’єктів: Монографія. К.: НАУ, 2016. 324 с.

11. . Бобух А.О. Автоматизовані системи керування технологічними процесами: Навчальний посібник. Харків: ХНАМГ, 2006. 185 с.

12. Пупена О.М. Розроблення людино-машинних інтерфейсів та систем збирання даних з використанням програмних засобів SCADA/HMI: Посібник. Київ, Ліра-К, 2020. 594 с.

13. С.В. Бейцун. Основи комп’ютерно-інтегрованого управління: Конспект лекцій та методичні вказівки до індивідуального завдання. Днепропетровск : НМетАУ, 2009. 45с

14. Головко Д.Б., Рего К.Г., Скрипник Ю.О. Автоматика і автоматизація технологічних процесів: Підручник. К.: Либідь, 1997. 232 с

15. О.П. Єгоров, М.О. Рибальченко, І.О. Маначин. Цифрові методи дослідження та розрахунку регуляторів в системах автоматичного керування : навчальний посібник. Дніпро : УДУНТ, 2022 .122 с