DOI 10.15276/imms.v11.no3.200
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 11 (2021), No. 3, pp. 200-208

СИСТЕМА МОДЕЛЮВАННЯ КІБЕРАТАКИ ПІДМІНОЮ OPC-СЕРВЕРА ПРИ КОМП'ЮТЕРНОМУ УПРАВЛІННІ ТЕХНОЛОГІЧНИМИ УСТАНОВКАМИ

А.А. Зозуля[1], О.А. Стопакевич[1], А.О. Стопакевич[2]

[1]Національний університет «Одеська політехніка»
1, пр. Шевченка, Одеса, 65044, Україна; e-mail: stopakevich@op.edu.ua
[2]Державний університет інтелектуальних технологій та зв'язку
1, вул. Кузнечна, Одеса, 65023, Україна; e-mail: stopakevich@gmail.com

Відповідно до звіту компанії Positive Technologies за вересень 2021р. 91% промислових компаній світу мають вразливі до кібератак інформаційні системи. Промисловий сектор – це другий за кількістю кібератак сектор в США, й ведучий в розвинутих країнах. Шосте й сьоме місце в топ двадцятці серед найбільших виробничих атак займає Україна. Сектору промислової кібербезпеки в світі присвячено багато наукових публікацій, але, нажаль, в Україні цією сферою кібербезпеки займаються слабо. Для розвитку тематики підвищення рівня кібербезпеки промислових систем керування, ми зосередились на проблемах кіберзахисту нижньої ланки керування – операторської станції керування технологічною установкою. Попередньо нами досліджена проблема кіберзахисту промислової комп'ютерної мережі нижчого рівня Modbus RTU. Продовжуючи тему, в цій роботі дослідитимо кібербезпеку важливого програмного забезпечення – OPC сервера. В дослідженні пропонується звернути увагу на вразливість, якої ще не досліджено. Ця вразливість зв'язана з тим, що маючи розгалужену мережу робочих станцій на підприємстві, зловмисник може підмінити OPC-сервер на будь якій робочій станції (зазвичай, найбільш важливій на виробництві) власним OPC-сервером і зробити таким чином, щоб з одного боку привести технологічний апарат обраної ділянки до зупинки чи аварії, а з другого боку, щоб оператор технологічної установки, спостерігаючи за SCADA-системою на екрані комп'ютера, нічого не помітив. Для виявлення кібератаки розроблено спеціальну діагностичну систему. Розроблено відповідне програмне забезпечення та, за його допомогою, всі рішення промодельовано в реальному часі з використанням компонентів реального промислового програмного забезпечення та моделі мережі Modbus. Розроблені рішення та програмне забезпечення можуть бути використані в промисловості.

Ключові слова: Кібератака, кіберзахист, OPC, OLE for Process Control, SCADA, система керування технологічною установкою.

Вступ

Відповідно до звіту компанії Positive Technologies [1] за вересень 2021 р. 91% промислових компанії світу мають вразливі до кібератак інформаційні системи. Промисловий сектор – це другий по кількістю кібератак сектор в США, й ведучий в розвинутих країнах. Шосте й сьоме місце в топ 20 серед найбільших успішних виробничих атак займає Україна. Відповідно, сектору промислової кібербезпеки в світі присвячено багато наукових публікацій, наприклад [2-5], але, нажаль, в Україні цією сферою кібербезпеки займаються слабо.

Для розвитку наукової теми підвищення кібербезпеки промислових систем керування ми зосередились на проблемах кіберзахисту нижньої ланки керування – операторської станції керування технологічною установкою. В роботі [6] нами було досліджено кіберзахист промислової комп'ютерної мережі нижчого рівня Modbus RTU. Продовжуючи тему, в цій роботі дослідимо проблему кібербезпеки важливого програмного забезпечення – OPC сервера.

Головною метою технології OPC [7] є забезпечення можливості спільної роботи засобів автоматизації, що функціонують на різних апаратних платформах, у різних промислових мережах та вироблених різними фірмами. До поширення технології OPC

з'єднання SCADA системи з кожних засобом автоматизації проводилось індивідуально. Існували довгі списки "підтримуваного обладнання", дуже складною була технічна підтримка. При модифікації обладнання потрібно було вносити зміни до всіх драйверів, кожен з яких підтримував протокол обміну тільки з однією клієнтською програмою. Число таких драйверів доходило до сотень. Після появи OPC практично всі SCADA-пакети були перепроектовані як OPC-клієнти, а кожен виробник апаратного забезпечення став постачати свої контролери, модулі вводу-виводу, інтелектуальні давачі та виконавчі пристрої зі стандартним OPC-сервером. Завдяки появі стандартизації інтерфейсу стало можливим підключення будь-якого фізичного пристрою до будь-якої SCADA, якщо вони відповідали стандарту OPC. Розробники отримали можливість проектувати лише один драйвер для всіх SCADA-пакетів, а користувачі отримали можливість вибору обладнання та програм без колишніх обмежень на їхню сумісність.

Приклад архітектури систем, що включають OPC-сервери та OPC-клієнти, показано на рис. 1. За наявності кількох операторських робочих станцій кожна з них може містити OPC-сервер та підключені до нього фізичні пристрої. У такій системі будь-який OPC-клієнт з будь-якого комп'ютера може звертатися до будь-якого OPC-серверу, у тому числі розташованого в іншій комп'ютерній мережі. Це досягається завдяки технології DCOM, яка використовує віддалений виклик процедур (RPC – Remote Procedure Call). Наприклад, технологічна установка 3 під керуванням SCADA-системи на рис. 1 може завдяки RPC звернутися й отримати дані зі SCADA-системи, яка керує установкою 1, що вказано штриховою лінією. Звернемо увагу, що комп'ютери та контролери у такій архітектурі можуть працювати з різними промисловими мережами. Обмін даними з ПЛК виконується точно так, як із комп'ютерами. OPC-сервер монопольно займає COM-порт (RS485) комп'ютера (оскільки безперервно виконує оновлення даних), тому кількість портів має дорівнювати кількості OPC серверів.

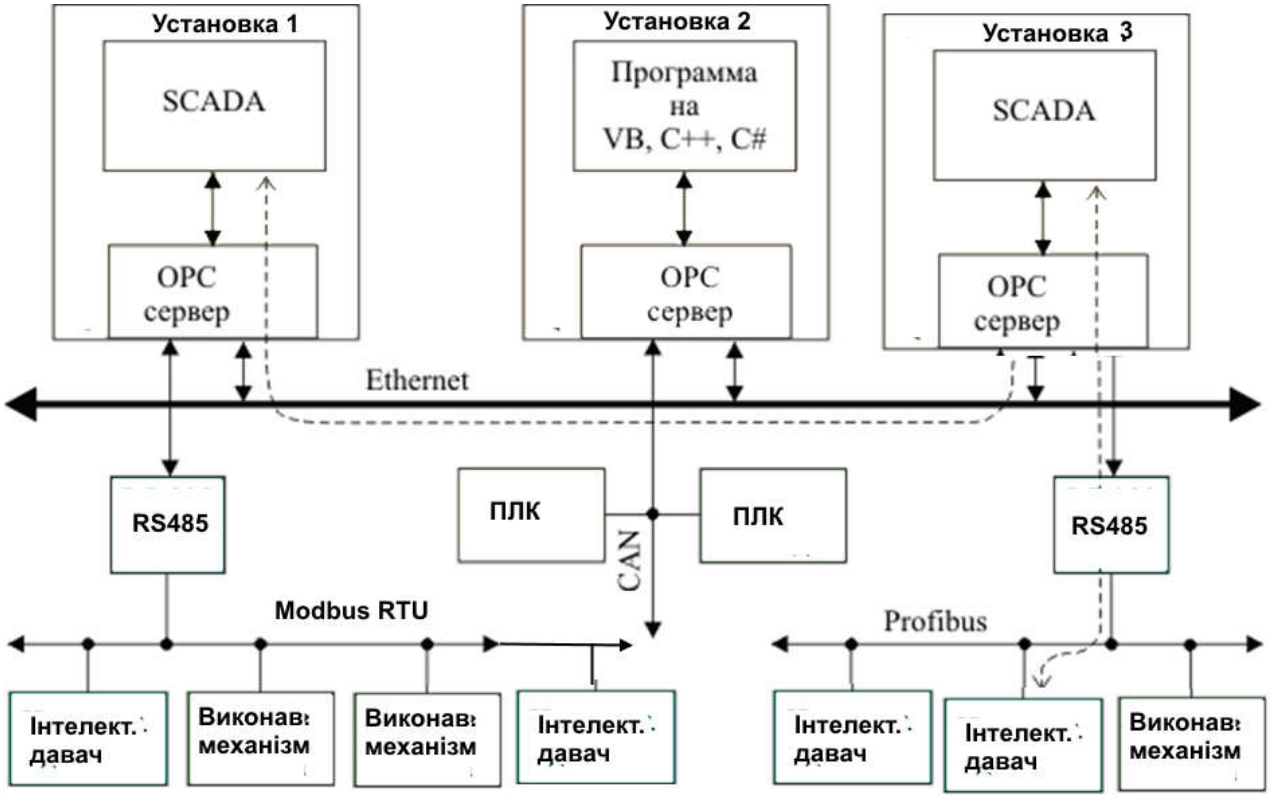

Рис. 1. Приклад використання OPC технології в системах автоматизації

Згідно аналітичному звіту [8] в програмному забезпеченні промислових систем керування знайдені вразливості, перелічені в табл.1.

В дослідженні пропонується звернути увагу на вразливість, яку ще не досліджено. Ця вразливість зв'язана з тим, що маючи розгалужену мережу робочих станцій на підприємстві, зловмисник може підмінити OPC сервер на будь якій робочій станції (зазвичай, найбільш важливій на виробництві) власним OPC-сервером і зробити таким чином, щоб з одного боку привести технологічний апарат обраної ділянки до зупинки чи аварії, а з другого боку, щоб оператор технологічної установки спостерігаючи за SCADA-системою на екрані комп'ютера нічого не помітив.

Таблиця 1

Кількість основних вразливостей, які знайдені розробниками звіту [8] за рік в програмному забезпеченні промислових систем керування, та умовний рівень їх небезпеки

№	Найменування вразливості	Кількість вразливостей	Рівень небезпеки
1	Переповнення буфера	17	**2**
2	Міжсайтові скрипти	14	**2**
3	Вразливості обходу аутентифікації	14	**2**
4	Жорстко закодовані облікові дані	9	**2**
5	Неправильна перевірка введення	9	**2**
6	Вразливості при передачі конфіденційної інформації	8	1
7	Зберігання паролів	6	**2**
8	Необмежене завантаження файлу	5	**2**
9	Ін'єкція SQL	5	**2**

Основна частина

Для моделювання обрано технологічний процес ректифікації суміші ізопропіла з водою [9]. Структура комп'ютерної системи керування відповідає структурі установки 1 на рис. 1. В програмному забезпеченні моделюється система керування з ПІ-регуляторами, яка налаштована за принципами, описаними в роботі [10] і описується математичною моделлю, зображеною на рис.2.

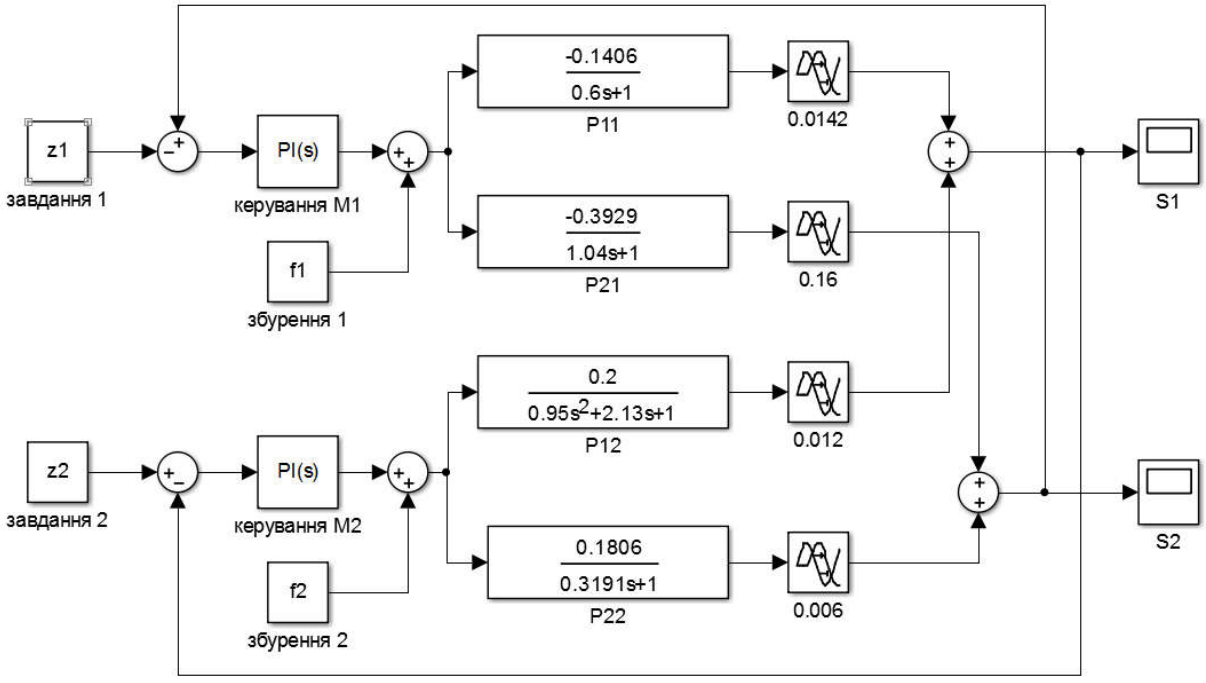

Рис. 2. Модель система керування ректифікаційною колоною (час в хвилинах)

Керовані змінні – температури зверху та знизу колони. Керуючі впливи – витрати пари і флегми (готового продукту, який повертається до колони для покращення розділення). S1 – це давач температури зверху, S2 – давач температури знизу, M1 – виконавчий механізм витрати флегми, M2 – виконавчий механізм витрати пари. Давачі і виконавчі механізми моделюються відповідно до технічної документації давачей типу TXTMINI-M12-485 і виконавчих механізмів TMB1-RTI Modbus Control Board for Electric Actuators. Бажаними показниками якості ходу технологічного процесу є підтримання температури зверху близької до 50 ^{o}C, температури знизу близької до 70^{o}C. На технологічний процес діють збурення за живленням колони, тому використовується автоматичне керування.

Для початку моделювання системи кібербезпеки запустимо симулятор технологічного процесу. Симулятор написано мовою програмування Python. Технологічний процес і пристрої керування, які працюють за протоколом Modbus, моделюються в реальному часі. В якостті емулятора нуль-модемного з'єднання використовується програма com0com.

Temperature Top : 50.0 Deg C

Temperature Btm : 70.0 Deg C

Reflux VLV : 50.0 %

Steam VLV : 50.0 %

	S1	S2		M1	M2
00	60001	60002	00	0	0
01	30001	30001	01	10	10
02	100	100	02	0	0
03	10	10	03	0	0
05	500	700	05	0	0
07	3	3	07	10	10
08	0	0	08	500	500
09	1	1	10	500	500
10	0	0	11	60	60
11	0	0	12	300	300
12	0	0	13	5	5
13	0	0	14	1000	1000
22	5	5	15	500	500

Column is operating in normal mode

Legend: Primary RW | Primary R | Secondary RW

Version: 0.10, Uptime: 0:00:03.022389
Port: COM4, Baud: 9600, Parity: None, XonXoff: False, StopBits:1

Рис. 3. Симулятор технологічного процесу для моделювання системи кібербезпеки

Основним робочим регістром давачей є регістр 5, який зберігає значення вимірювань як ціле число. Наприклад, 500 – це 50.1 ^{o}C. Для виконавчих механізмів найважливішими є три регістри. Регістр 0 вказує переміщення виконавчого механізму – значення 0 означає, що немає переміщення; 64 – переміщення за часовою стрілкою; 128 – переміщення проти часової стрілки. Регістр 8 зберігає поточне положення регулюючого органу, яке вимірюється давачем положення. Регістр 10 використовується для задавання нового положення. Значення в регістрах теж цілочислове.

Для реалізації зв'язку промислової мережі Modbus і комп'ютерної мережі використано популярний OPC-сервер фірми Insat (рис. 4). Сервер з'єднується з емулятором за допомогою нуль-модемного з'єднання. Кожен важливий параметр має свій відповідник –

тег, тобто структуровану змінну, значення якої прив'язано до певного регістру і масштабується сервером.

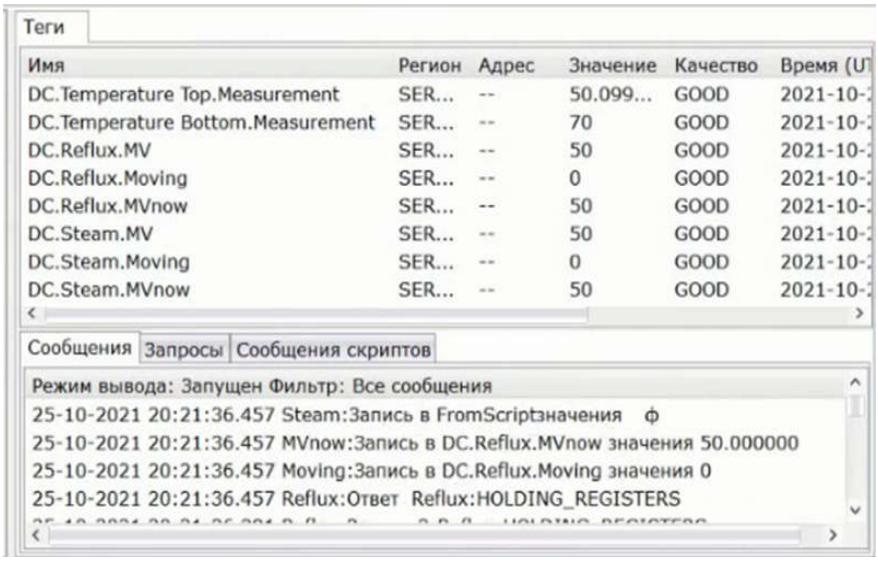

Рис. 4. Копія головного вікна OPC-серверу

OPC-сервер є одним з вразливих елементів системи автоматизації, оскільки доступ до нього можуть мати всі комп'ютери мережі. Сам сервер має програмний інтерфейс за допомогою якого програмісти можуть змінювати його поведінку в реальному часі. Таким чином, можливо, наприклад, сфальсифікувати параметри. Захист від такої фальсифікації – актуальна задача.

Розглянемо як мету хакерської атаки зупинку технологічного процесу. Для цього хакеру необхідно відключити автоматичне керування і вивести витрату флегми та пари на 100% відкриття.

Запустимо комп'ютерне програмне забезпечення системи керування – SCADA-систему (рис. 5). Ця система реалізує процес керування і людино-машинний інтерфейс. Зв'язок з промисловою мережею в SCADA-системі реалізується за допомогою OPC-серверу. Вважаймо, що доступ до SCADA-системи хакер не має.

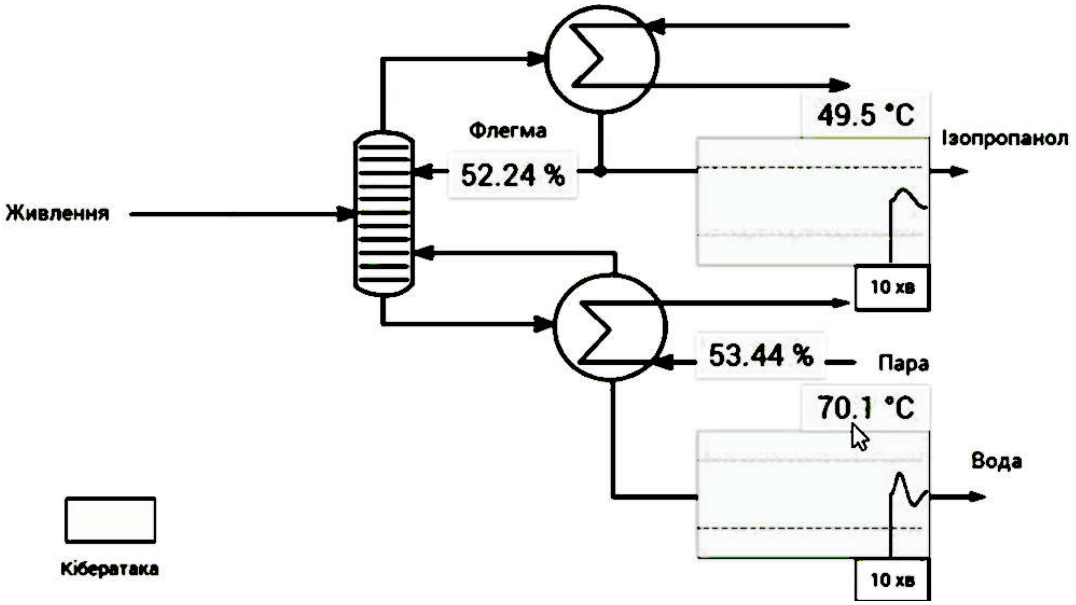

Рис. 5. Форма оператора-технолога в SCADA-системі

Дочекаємось часткової стабілізації параметрів технологічного процесу. Бачимо за трендами, що регулятори реалізують автоматичне керування.

Метою хакера є створити видимість того, що автоматичне керування продовжується і змінні більш-менш в регламентних межах. В той же час значення не мають бути постійними, бо для оператора технологічної установки це буде дуже помітним.

Хакер не має моделі технологічного процесу і не знає налаштувань регуляторів, тому для нього єдиним виходом щоб не видати себе є програмна імітація достатньо реалістичного продовження ходу технологічного процесу після зламу таким чином, щоб регулятори за заданий час не вийшли за регламентні межі. Це він реалізує шляхом заміни OPC-серверу на такий же, але перепрограмований під фальсифікацію показань давачей і положень виконавчих механізмів.

Проведемо підміну OPC-сервера, запустивши скрипт hack з командної консолі Windows (рис. 6).

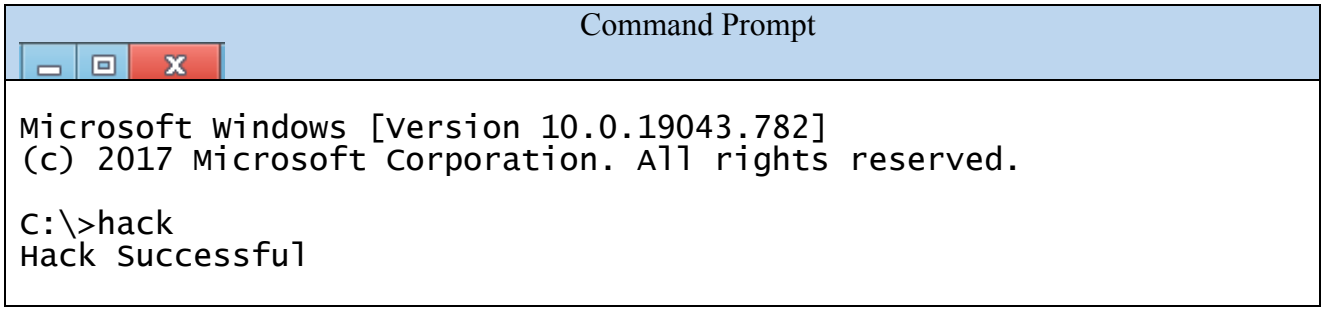

Рис. 6. Введення команди для зламу

Після цього станеться неконтрольоване збільшення положення виконавчих механізмів (бачимо що завдання на реальне положення виконавчих механізмів встановлені на 100% відсотків у вікні симулятора на рис. 7). Але на формі SCADA-системи цього помітно не буде (рис. 5).

	S1	S2		M1	M2
08	0	0	08	710	710
09	1	1	10	1000	1000

Рис. 7. Значення регістрів в симуляторі після зламу

В програмному забезпеченні SCADA-системи працює алгоритм виявлення зламу. Сутність цього алгоритму полягає в тому, що для кожного регулятору розраховується різниця між поточним й попереднім (секунду назад) значенням керуючого впливу. Якщо $u_i - u_{i-1} > 0$ і значення регістру 0 дорівнює 64, або $u_i - u_{i-1} < 0$ і значення регістру 0 дорівнює 128, або $u_{i-1} = 0$ і значення регістру 0 дорівнює 0, то процес керування йде вірно. При порушенні будь-якого з цих умов підраховується кількість таких порушень і якщо вона перевищує порогове значення (прийнято 10 підряд), то спрацьовує сигналізація в SCADA-системі (червоний прямокутник) й оператору передається повідомлення про хакерську атаку.

Бачимо, що OPC-сервер передав у промислову мережу значення керуючих впливів, яке дорівнює 100% (рис. 7). Відлік часу до порушення роботи колони почався. Програмне забезпечення, реалізоване в SCADA має виявити нестандартну поведінку. Критерієм нестандартної поведінки є відсутність руху регулюючого органу при підтверджені зміни положення.

На формі SCADA-системи бачимо, що процес для оператора установки висвітлюється як нормальний (рис.8). Але розроблена система діагностики виявила злам і пропонує оператору технологічної установки зупинити OPC-сервер. Це він повинен зробити з допомогою спеціальної кнопки. Після її натискання оператором OPC-сервер буде зупинено разом зі SCADA-системою.

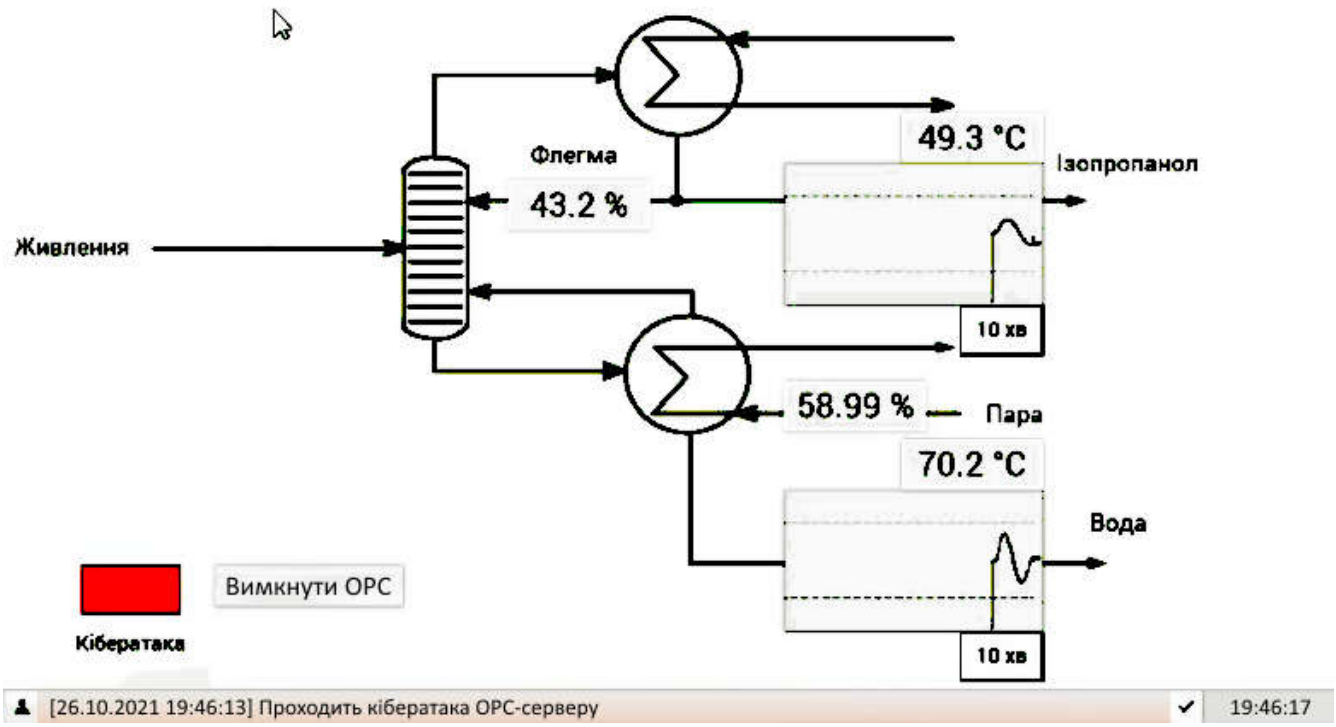

Рис. 8. Екран SCADA-системи після діагностування кібератаки

Після відімкнення SCADA-системи адміністратор мережі має повернути положення регулюючих органів за допомогою команд Modbus чи оператор технологічної установки має повернути положення регулюючих органів вручну за допомогою ручного дублера, який встановлений на кожному регулюючому органі. Далі системний адміністратор мережі повинен зрозуміти знаходження джерела зламу, усунити його та відновити роботу оригінального ОРС-серверу. Після цього SCADA-систему треба запустить знову.

Висновки

Викрито можливість нової кібератаки на робочі станції керування технологічними установками промислових процесів. Сенс кібератаки полягає в тому, що по мережі, яка зв'язує технологічні станції, робиться підміна ОРС-сервера, після чого технологічна установка зловмисником переводиться в аварійний стан таким чином, щоб оператор, спостерігаючи за технологічним процесом за допомогою SCADA-системи не міг помітити розбалансування процесу. Для виявлення кібератаки розроблено спеціальну діагностичну систему. Розроблено відповідне програмне забезпечення та, за його допомогою, всі рішення промодельовано в реальному часі з використанням компонентів реального промислового програмного забезпечення та моделі мережі Modbus. Розроблені рішення та програмне забезпечення можуть бути використані в промисловості.

Список літератури

1. Information security risks at industrial companies. Moscow: Positive Technologies, 2021. 7p.
2. Zegzhda D.P., Kalinin M.O., Levykin M.V. Actual Vulnerabilities of Industrial Automation Protocols of an Open Platform Communications Series. *Automatic Control and Computer Sciences,* 2019. Vol. 53, No. 8, pp. 972–979
3. Candell R., Anand D.M., Stouffer K. A Cybersecurity Testbed for Industrial Control Systems. *ISA Process Control & Safety Symposium.* Texas, Houston: ISA, 2014. 16p.
4. Adeyanju1 I.A, Emake E.D., Olaniyan O.M., Omidiora E.O., Adefarati T., Uzedhe G.O., Okomba N.S. Digital Industrial Control Systems: Vulnerabilities and Security Technologies. *Current Applied Science and Technology.* Vol. 21. No. 1. P. 185–200.
5. Alves T., Das R., Morris T. Virtualization of Industrial Control System Testbeds for Cybersecurity. *ICSS '16.* Los Angeles, CA: ACM, 2016. P.1-19
6. Зозуля А.А., Стопакевич О.А. Вдосконалення протоколу Modbus RTU з метою підвищення кіберзахищенності комп'ютерно - інтегрованої АСУТП. *62 Міжнародна наук. конф.«Актуальні наукові дослідження в сучасному світі»*. Переяслав, 2020. Вип. 6 (62). Ч. 2. С. 49-53.
7. Энциклопедия АСУ ТП. OPC сервер. URL:https://www.bookasutp.ru/chapter9_2.aspx
8. Andreeva O., Gordeychik S., Gritsai G., Kochetova O., Potseluevskaya E., Sidorov S., Timorin A. Industrial control systems vulnerabilities statistics. Moscow: Kaspersky Lab, 2015. 18p.
9. Yadav E.S., Indiran T., Priya S.S., Fedele G. Parameter Estimation and an Extended Predictive-Based Tuning Method for a Lab-Scale Distillation Column. *ACS Omega*, 2019. Vol. 4, No. 25. P. 21230–21241.
10. Stopakevych, A., Stopakevych, O. Design of robust controllers for plants with large dead time. *Eastern-European Journal of Enterprise Technologies*, 2016. Vol. 1. No. 2. P. 48-56. https://doi.org/10.15587/1729-4061.2016.59107

SIMULATION SYSTEM OF CYBERATTACK BY OPC SERVER REPLACEMENT IN COMPUTER CONTROL SYSTEMS OF TECHNOLOGICAL PLANTS

A.A. Zozulya, O.A. Stopakevich, A.O. Stopakevich

National Odessa Polytechnic University
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: stopakevich@gmail.com

According to a September 2021 report by Positive Technologies, 91% of the world's industrial companies have information systems vulnerable to cyberattacks. The industrial sector is the second most attacked sector in the U.S., and the leading one in developed countries. Ukraine ranks sixth and seventh in the top 20 for the largest industrial attacks. Many scientific publications are devoted to industrial cybersecurity in the world, but, unfortunately, in Ukraine this area of cybersecurity is poorly studied. To develop the topic of increasing the level of cybersecurity of industrial control systems, we focused on the problems of cybersecurity of the lower level of control - the operator control station of the technological plant. Previously, we investigated the problem of cybersecurity of the industrial computer network of the lower level Modbus RTU. Continuing the topic, in this paper we investigate the cybersecurity of important software - the OPC server. This study proposes to pay attention to a vulnerability that has not yet been investigated.This vulnerability is related to the fact that having an extensive network of workstations in the enterprise, an attacker can substitute OPC server on any workstation (usually the most important one in production) with his own OPC server and do it in such a way that on the one hand to bring the technological unit of the selected site to stop or crash, but on the other hand to prevent the operator of technological unit, watching the SCADA-system on the computer screen, from noticing anything. A special diagnostic system has been developed to detect a cyber attack. Appropriate software has been developed and, with its help, all solutions have been simulated in real time using components of real industrial software and Modbus network model. The developed solutions and software can be used in industry.

Keywords: Cyber-attack, cyber defense, OPC, OLE for Process Control, SCADA, process control system.