УДК 621.317.73

THE CURRENT STATE AND ANALYSIS OF CYBER SECURITY OF PROCESS CONTROL SYSTEM AND AUTOMATED MANUFACTURING MANAGEMENT SYSTEM

A. Mykhaliuk, R. Mirkevych
National University of Food Technologies

Key words:
SCADA cloud systems
Cyberattacks
Vulnerabilities
Network IDS/IPS
Insider threats
Supply chain security

Article history:
Received 11.07.2024
Received in revised form 30.07.2024
Accepted 14.08.2024

Corresponding author:
A. Mykhaliuk
E-mail:
andrew.mikhaliuk@corewin.ua

Citation: Михалюк А. П., Міркевич Р. М. (2024). Сучасний стан та аналіз кібербезпеки автоматизованих систем керування технологічними процесами та автоматизованих систем управління виробництвом. *Наукові праці НУХТ*, 30(4), 7—30.
DOI: 10.24263/2225-2924-2024-30-4-3

ABSTRACT

Vulnerabilities and cyberattacks that threaten the security of cloud-based SCADA (Supervisory Control and Data Acquisition) systems are analyzed in this study. Four key areas of vulnerability were identified that are critical to the functioning of these systems: communication between SCADA systems and cloud services, shared infrastructure, the possibility of insider attackers, and the robustness of SCADA protocol security.

Cyberattacks were classified into five main groups, including attacks on hardware, software, communication and protocols, management processes, and insider attacks. DoS (Denial of Service), MITM (Man-In-The-Middle) and APT (Advanced Persistent Threat) were identified as the most significant threats to cloud SCADA systems. To mitigate these threats, it is recommended using network IDS/IPS (Network Intrusion Detection Systems/Network Intrusion Prevention Systems, NIDS/NIPS).

However, some threats remain insufficiently addressed. Sophisticated malware, insufficient IoT (Internet of Things) security and reliance on cloud providers, and supply chain vulnerabilities pose additional risks to SCADA systems. There is particularly dangerous concept of competitive artificial intelligence, which can deceive security systems or carry out attacks on SCADA systems.

Measures to improve the security of cloud-based SCADA systems: implementing real-time security monitoring systems, developing robust incident response plans, regular security audits, improving IoT security, and working closely between different organizations to share threat information were also recommended.

In addition, the security of cloud-based SCADA systems requires further research to prevent future incidents and catastrophic events. In particular, potential quantum attacks and supply chain security need to be investigated, as these aspects may significantly affect the stability and security of SCADA systems in the future.

DOI: 10.24263/2225-2924-2024-30-4-3

СУЧАСНИЙ СТАН ТА АНАЛІЗ КІБЕРБЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ КЕРУВАННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ ТА АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ВИРОБНИЦТВОМ

А. П. Михалюк, Р. М. Міркевич
Національний університет харчових технологій

У цьому оглядовому дослідженні аналізувалися вразливості та кібератаки, що загрожують безпеці хмарних систем SCADA (Supervisory Control and Data Acquisition). Виявлено чотири ключові області вразливості, що мають вирішальне значення для функціонування цих систем: зв'язок між системами SCADA та хмарними службами, спільна інфраструктура, можливість присутності зловмисників-інсайдерів і надійність безпеки протоколів SCADA.

Кібератаки класифікувалися на п'ять основних груп, що включають атаки на апаратне забезпечення, програмне забезпечення, зв'язок і протоколи, процеси керування й атаки зсередини. Найбільш значущими загрозами для хмарних систем SCADA були визначені DoS (Denial of Service), MITM (Man-In-The-Middle) та APT (Advanced Persistent Threat). Для пом'якшення цих загроз рекомендується використовувати мережеві IDS/IPS (Network Intrusion Detection Systems/Network Intrusion Prevention Systems, NIDS/NIPS).

Проте деякі загрози залишаються недостатньо вирішеними. Складне шкідливе програмне забезпечення, недостатня безпека IoT (Internet of Things) та залежність від постачальників хмарних технологій і вразливості в ланцюгу постачання створюють додаткові ризики для SCADA-систем. Особливо небезпечною є концепція змагального штучного інтелекту, що може обманювати системи безпеки або здійснювати атаки на SCADA-системи.

У дослідженні також рекомендуються заходи для підвищення безпеки хмарних систем SCADA: впровадження систем моніторингу безпеки в реальному часі, розробка надійних планів реагування на інциденти, регулярні перевірки безпеки, підвищення безпеки IoT і тісна співпраця між різними організаціями для обміну інформацією про загрози.

Крім того, безпека хмарних систем SCADA вимагає подальших досліджень для запобігання майбутнім інцидентам і катастрофічним подіям. Зокрема, необхідно дослідити потенційні квантові атаки та безпеку ланцюга постачання, оскільки ці аспекти можуть суттєво вплинути на стабільність і захищеність SCADA-систем у майбутньому.

Ключові слова: *хмарні системи SCADA, кібератаки, вразливості, мережеві IDS/IPS, внутрішні загрози, безпека ланцюга постачання.*

Постановка проблеми. Диспетчерське керування та збір даних (SCADA) являє собою архітектуру системи керування, необхідну для роботи критичної інфра-

структури в промислових секторах, включаючи виробництво електроенергії, видобуток нафти, газу та виробничі підприємства, зокрема й підприємства харчової промисловості. Ці системи полегшують роботу, контролюючи та відстежуючи дані та процеси в реальному часі, локально або віддалено. Вони використовують різні компоненти, такі як датчики, приводи, перемикачі й клапани (Morsey, 2017). Системи SCADA перейшли від автономних, ізольованих середовищ (наприклад, монолітних або розподілених) з обмеженими функціями та власними протоколами зв'язку до мережевих платформ, що використовують глобальні мережі (WAN) з відкритими протоколами та стандартами зв'язку (Yadav, & Paul, 2021). Натепер системи SCADA перетворилися на відкриті системи, підключені до Інтернету, повністю інтегровані з мережами корпоративних інформаційних технологій (IT) і підтримують різні засоби, програмне забезпечення та Інтернет-протоколи, такі як TCP/IP (Yadav, & Paul, 2021; Cai, Wang, & Yu, 2008). Такий рівень інтеграції підвищив продуктивність та функціональні можливості SCADA систем, але в той же час зробив системи цього рівня вразливими для кібератак. Пропоноване дослідження присвячене огляду сучасного стану кібербезпеки в автоматизованих системах керування.

Аналіз останніх досліджень і публікацій. Оскільки складні промислові операції вимагають передових і ефективних середовищ та обробляють величезні обсяги даних, у літературі пропонується перенести системи SCADA в хмару (Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019). Хмарні обчислення, що використовують паралельні та розподілені системи, пропонують IT-ресурси за конкретними угодами про рівень обслуговування між клієнтами й постачальниками послуг (Buyya, Yeo, & Venugopal, 2008). Хмарні системи можуть підвищити продуктивність традиційних систем за рахунок зниження технічних і промислових витрат. Ці складні системи покращують характеристики обчислювального середовища, зокрема якість обслуговування, надійність, гнучкість і ефективність зв'язку. Крім того, вони забезпечують відповідну конфігурацію та обслуговування системи (Mushtaq та ін., 2017).

Існують два методи інтеграції систем SCADA з технологіями хмарних обчислень (Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019).

Перший метод передбачає використання загальнодоступної хмарної інфраструктури, де програми SCADA виконуються в приміщеннях компаній або організацій. Хоча функції керування додатками SCADA залишаються ізольованими в мережі контролера, вони безпосередньо підключені до хмарних служб для передачі, зберігання та розподілу даних.

Другий метод використовує приватну або гібридну хмарну інфраструктуру, в якій додатки SCADA повністю виконуються в хмарі, а контролери віддалено підключаються до цих додатків через з'єднання WAN. Важливо, що забезпечення надійних заходів безпеки, мінімальної затримки та високої доступності послуг має вирішальне значення при переході критичної інфраструктури SCADA до хмарного середовища (Tariq, Asim, & Khan, 2019).

Хоча використання хмарних систем SCADA зростає в різних галузях промисловості, ці системи стикаються з тими ж проблемами кібербезпеки, що й інші системи, інтегровані в хмару. Дані в хмарі часто доступні та знаходяться у відкритому, розподіленому середовищі (Church та ін., 2017). Функції хмарних систем

SCADA, такі як моніторинг у реальному часі та/або контроль процесів, передача даних через Інтернет і віддалений доступ, створюють численні вразливості безпеки, якими можуть скористатися потенційні зловмисники. Ці вразливості дають змогу зловмисникам впроваджувати небезпечне програмне забезпечення, змінювати контрольні дані або блокувати передачу даних (Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019). Крім того, публічне хмарне середовище наражає ці системи на інші загрози безпеці, включаючи атаки на відмову в обслуговуванні (DoS), розподілені DoS (DDoS) й атаки типу «людина посередині» (MITM) (El Mrabet, Kaabouch, El Ghazi, & El Ghazi, 2018).

Дослідники в попередніх дослідженнях детально розглянули хмарні структури SCADA та їх основні компоненти, як зазначено в посиланнях (Church та ін., 2017; Church та ін., 2015; Wilhoit, 2013; Yi, Mueller, Yu, & Chuan, 2017). Однак за останні роки існує обмежена кількість наукових досліджень, присвячених проблемам безпеки, властивим цим ключовим інфраструктурам. Щоб згадати деякі з них, автори (Bhamare та ін., 2020; Alakbarov, & Hashimov, 2023) загалом розглядали широкі вразливості та кібератаки хмарних систем SCADA, включаючи обмежений контроль безпеки над даними, втрату з'єднання, відсутність стандартизації безпеки та відсутність достатньої автентифікації та механізми шифрування. Дослідники пропонують різні заходи кібербезпеки, такі як шифрування, системи виявлення вторгнень і розробка безпечної архітектури для виявлення та пом'якшення кіберзагроз у хмарних середовищах. Крім того, у статті (Alakbarov, & Hashimov, 2023) підкреслюється важливість регулярного аналізу журналів, застосування рішень безпеки на основі блокчейну для покращення цілісності та контролю даних, а також необхідність ретельного резервного копіювання та відновлення даних. У системах присутні вразливі місця та загрози системам SCADA у хмарних середовищах Інтернету речей (IoT) (Sajid, Abbas, & Saleem, 2016), включаючи ризики безпеки, пов'язані з реєстрацією даних, відсутністю механізмів автентифікації та шифрування, а також загрози відсутності захисту вбудованих пристроїв, в основі промислових систем SCADA на основі IoT.

Інші дослідження класифікують різні атаки на основі конкретних критеріїв. Загрози для критичної інфраструктури, представляючи різні атаки на системи SCADA, аналіз атак на критичну інфраструктуру та вектори атак з підтримкою IoT, включаючи їхній вплив на охорону здоров'я, транспортні системи та стільникову інфраструктуру 5G присутні у авторів по цій темі (Maglaras та ін., 2018). Для захисту критично важливих інформаційних активів у документі описано заходи кібербезпеки, класифіковані відповідно до правових, технічних, організаційних аспектів, аспектів нарощування потенціалу та співпраці. Він підкреслює важливість розвідки кіберзагроз для превентивних заходів протидії потенційним атакам.

Автори рекомендують вивчати нові протоколи SCADA, розроблені для задоволення вимог Industry 4.0, інтегрувати концепції IoT, використовувати технології віртуалізації, такі як Software Defined Networking (SDN) і Network Function Virtualization (NFV), застосування аналітики великих даних для підвищення безпеки SCADA та прийняття структури кібергігієни SCADA (Pliatsios, Sarigiannidis, Lagkas, & Sarigiannidis, 2020). Подібним чином у статті (Ghosh, & Sampalli, 2019) представлено класифікацію атак на основі потреб безпеки та рівнів мережевого

протоколу систем SCADA. Ця класифікація охоплює атаки на апаратне забезпечення, програмне забезпечення та мережеві з'єднання. У ньому розглядаються численні схеми безпеки, запропоновані для усунення вразливостей мережі SCADA, організовуючи їх на основі поточних стандартів, виявлення та запобігання атакам.

Метою дослідження є огляд, аналіз і дослідження сучасного стану інформаційної безпеки автоматизованих систем керування технологічними процесами й автоматизованих систем управління об'єктів критичної інфраструктури та виробничих підприємств, зокрема підприємств харчової промисловості.

Матеріали і методи. Використані сучасні наукові матеріали, у яких досліджується використання методів інформаційної безпеки автоматизованих систем керування. Як методичне забезпечення застосовано практичні інженерні методи розробки та імплементації автоматизованих систем керування технологічними процесами й виробництвами з урахуванням вимог інформаційної безпеки, описані в таких міжнародних і галузевих технічних стандартах, як серія стандартів IEC 62443-2-1 (ISA-99).

Викладення основних результатів дослідження. Загалом, обсяг існуючих досліджень безпеки хмарних систем SCADA часто звужується до конкретних типів атак, а результати розкидані по численних публікаціях. Усуваючи цю прогалину, наше дослідження має на меті запропонувати всебічний огляд основних вразливостей і кібератак, спрямованих на хмарні системи SCADA. Крім того, буде розглянуто ряд існуючих рішень безпеки, розроблених для посилення цих систем проти таких загроз.

Щоб зрозуміти вразливості та кібератаки, описані далі, пропонується короткий огляд архітектури традиційних і хмарних систем SCADA, а також основних технологій, які використовуються в обох системах.

Традиційні системи SCADA складаються з інтеграції апаратних компонентів, програмного забезпечення та каналів зв'язку, які полегшують моніторинг, контроль і управління промисловими процесами. Апаратне забезпечення включає віддалені термінали (RTU), програмовані логічні контролери (PLC), інтелектуальні електронні пристрої (IED), головні термінали (MTU), а також виконавчі пристрої та датчики. Програмне забезпечення охоплює людино-машинний інтерфейс (HMI), центральну базу даних (Historian) та інше програмне забезпечення користувача (Yadav, & Paul, 2021). RTU збирають дані в режимі реального часу від датчиків у фізичному середовищі через канали LAN/WAN і передають цю інформацію до MTU. Поряд з ПЛК та IED, RTU локально керують виконавчими механізмами та контролюють датчики SCADA (Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019). RTU також передають дані поточного стану підключених фізичних пристроїв. MTU діє як центральна станція моніторингу, видаючи команди RTU, відповідаючи на їхні повідомлення, обробляючи та зберігаючи дані, аналізуючи інформацію та створюючи звіти для майбутнього зв'язку.

HMI діє як інтерфейс між апаратним і програмним забезпеченням SCADA, полегшуючи контроль, моніторинг і зв'язок між RTU і MTU. Historian відповідає за зберігання даних зв'язку, подій і сигналів тривоги та виконує функції централізованої бази даних або сервера. Він підтримує HMI, надаючи дані для графічного аналізу трендів. Комунікаційна мережа забезпечує взаємодію між компонентами SCADA, використовуючи бездротові або дротові засоби масової інформації.

Часто перевагу надають бездротовому зв'язку через його ефективність у з'єднанні географічно розподілених і віддалених районів. Ця мережа, зазвичай, ізольована від зовнішніх мереж, щоб зменшити ризики кібербезпеки. Традиційні системи SCADA працюють незалежно на місці та часто використовують закриті, специфічні для постачальника та власні протоколи зв'язку в режимі реального часу (наприклад, TCP/IP, Modbus), які підвищують безпеку через невідомість, але можуть обмежити взаємодію. На рис. 1 показано загальну архітектуру традиційної системи SCADA. Для отримання додаткової інформації ми відсилаємо читача до (Yadav, & Paul, 2021; Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019).

Рис. 1. Архітектура традиційних систем SCADA

У хмарній системі SCADA архітектура, зазвичай, передбачає інтеграцію додатків SCADA з хмарними службами для підвищення масштабованості, доступності та рентабельності (Combs, 2011). На додаток до різних традиційних компонентів систем SCADA, хмарна архітектура відповідає за більш широку обробку даних, зберігання та розширену аналітику (Yadav, & Paul, 2021). Він забезпечує глобальний доступ до даних, підтримує масштабні обчислювальні завдання та розміщує додатки, які вимагають значної обчислювальної потужності. Контролери, такі як RTU та PLC, підключаються через канали WAN до програм SCADA, що виконуються в хмарі (Sajid, Abbas, & Saleem, 2016).

Хмарні системи SCADA включають інтеграцію Cyber-Physical Systems (CPS)/IoT, що забезпечує підключення широкого спектра датчиків і пристроїв та полегшує збір і автоматизацію даних у реальному часі. Сервіси хостингу, як-от туманні вузли, які включають промислові контролери, маршрутизатори та вбудовані сервери, діють як посередники, обробляючи дані ближче до їх джерела, щоб покращити обробку в реальному часі, зменшити затримку та підтримати локальну аналітику та зберігання даних (Yadav, & Paul, 2021; Byers, 2018). Крім того, функції керування в додатку SCADA відокремлені в мережі контролера, тоді як сам додаток підключено до хмарних служб для візуалізації, звітності та віддаленого доступу (Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019). Комунікаційні мережі в хмарних системах SCADA підтримують різні протоколи та стандарти (наприклад, протокол розподіленої мережі (DNP3)), забезпечуючи взаємодію та безпечний обмін даними між пристроями та хмарою (Nugent, 2017). Інфраструктура також інтегрує технології безпеки, такі як брандмауери, які контролюють

вхідний і вихідний мережевий трафік, і включає в себе шифрування, автентифікацію, системи виявлення вторгнень і механізми контролю доступу для захисту від кіберзагроз (Howard, 2015).

Загалом, системи хмарних обчислень пропонують чотири основні рівні послуг для додатків SCADA, кожен з яких структурований ієрархічно таким чином (Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019; Combs, 2011):

1. Апаратний рівень, розташований у центрах обробки даних, складається з основних фізичних компонентів, таких як процесори, пам'ять, сховище та пропускна здатність.
2. Рівень інфраструктури впроваджує віртуалізацію та надає інфраструктуру як послугу (IaaS), що містить пул віртуальних машин (VM), на яких розміщені програми SCADA і може бути наданий на вимогу IT-користувачам.
3. Рівень платформи базується на службах інфраструктури, щоб пропонувати платформу як послугу (PaaS), що дає змогу розробляти й доставляти програмне забезпечення через Інтернет.
4. Рівень програмного забезпечення надає готове до використання рішення та програми, що задовольняють різноманітні потреби бізнесу та надають програмне забезпечення як послугу (SaaS) за допомогою компонентів і служб рівня платформи.

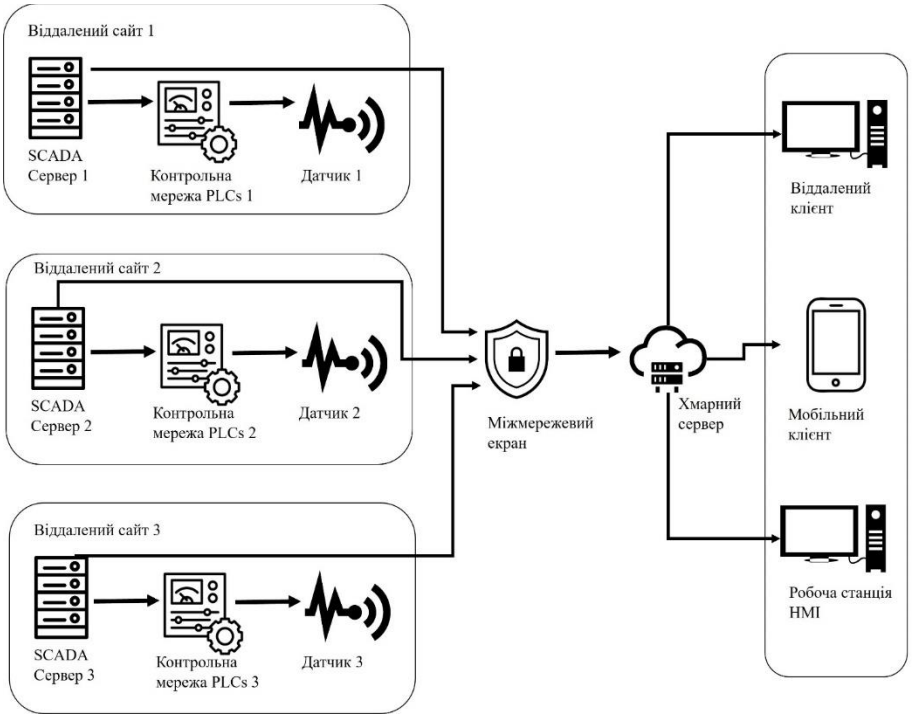

Рис. 2. Архітектура хмарних SCADA системи

Перехід до хмарних систем SCADA від традиційних архітектур знаменує значний зсув до більш інтегрованих, інтелектуальних і гнучких промислових систем

управління. Хоча хмарні системи пропонують численні переваги, вони також створюють нові проблеми, особливо щодо кібербезпеки та конфіденційності даних. В обох архітектурах наголос на безпеці (як за допомогою кібернетичних, так і фізичних засобів) залишається першочерговим, що підкреслює критичну важливість захисту промислових процесів та інфраструктури.

У результаті аналізу літературних джерел можна виділити чотири основні фактори вразливості:

- підключення до хмарних сервісів;
- спільна інфраструктура;
- шкідливі інсайдери;
- безпека протоколів SCADA.

Крім того, було окреслено п’ять категорій кібератак:

- апаратні;
- програмні;
- комунікаційні та протокольні;
- контрольні атаки;
- інсайдерські атаки.

У межах цих атак на програмне забезпечення додатково класифікуються як промислові системи управління (ICS), які засновані на вразливостях або специфічні для хмари. Найпоширенішими тактиками під час різноманітних кібератак, що впливають на безпеку хмарних систем SCADA, є DoS, MITM і атаки на розширені стійкі загрози (APT). Рис. 3 ілюструє загальну класифікацію факторів вразливості, кібератак і їх загальну тактику, отриману з підходу індуктивного узагальнення, застосованого до відповідних досліджень. Також у цьому документі обговорюються кілька відповідних рішень безпеки для хмарних обчислень загалом і хмарних систем SCADA зокрема, рекомендовано їх застосування для виявлення та запобігання кібератак.

Попередні дослідження вивчали загальні фактори вразливості та проблеми безпеки в хмарних системах SCADA. Ці виклики варіюються від людських помилок і недостатніх ресурсів для фізичних пристроїв до власних протоколів і незахищених застарілих систем. Незахищені застарілі інтерфейси керування, підключення до Інтернету, підключені промислові пристрої Інтернету речей (IIoT) і різноманітні пристрої, які можна взяти з собою (BYOD) (Mesbah, Elsayed, Jurcut, & Azer, 2023), разом із нещасними випадками через недбалість і збої обладнання (Rakas, Stojanović, & Marković-Petrović, 2020), все це може служити точками входу в системи для кібератак, введення вразливостей. Крім того, незахищені віртуальні машини, недоступність хмарної інфраструктури (Nazir, Patel, & Patel, 2020), викрадення облікового запису або трафіку служби (Cerullo, Mazzeo, Papale, Sgaglione, & Cristaldi, 2016), проблеми з безпекою промислової автоматизації та пристроїв аналізу, невідповідні механізми безпеки програмного забезпечення в багатьох промислових датчиках, що виконують процеси в реальному часі (Mesbah, Elsayed, Jurcut, & Azer, 2023), а також відсутність належних бекдор-можливостей деякими виробниками для керування та оновлення промислових пристроїв (Ulltveit-Moe та ін., 2016) є значними факторами вразливості, які організації повинні враховувати після переходу на хмарну інфраструктуру.

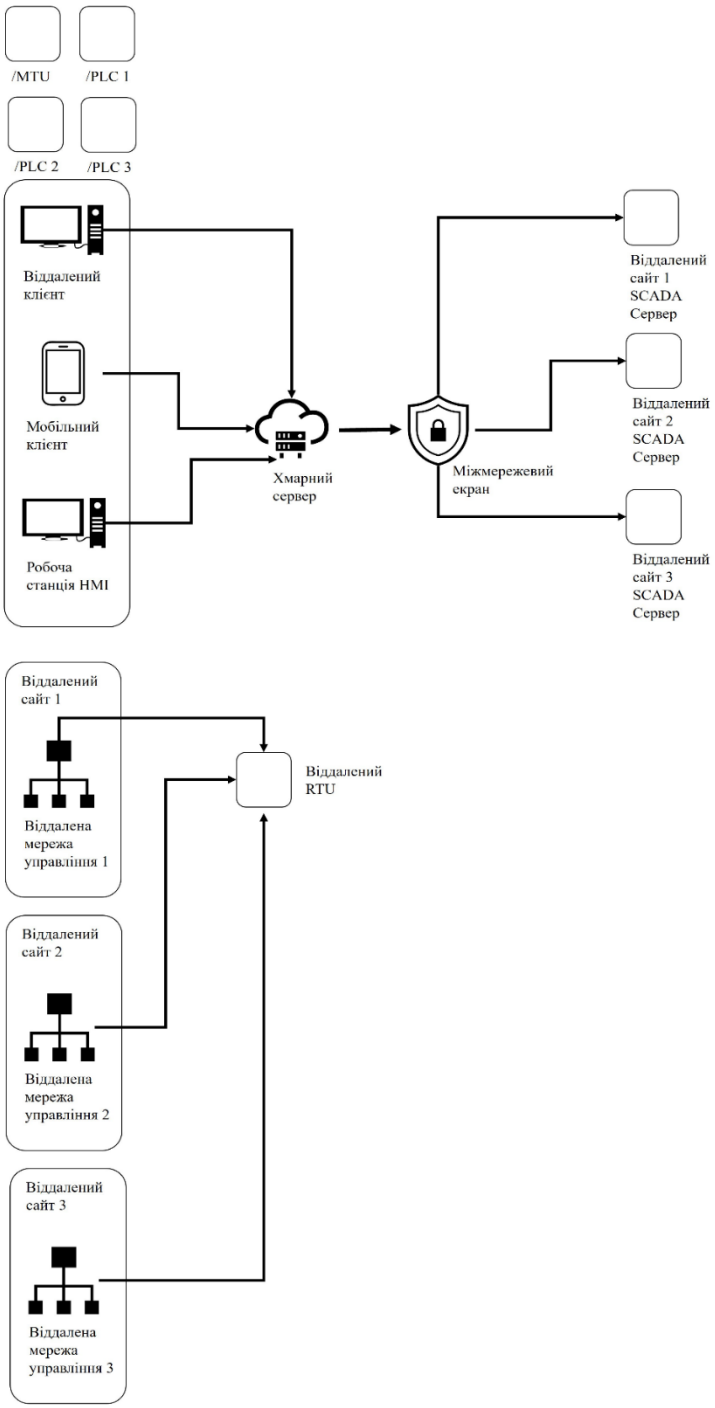

Рис. 3. Промислова система управління (ICS) з інтеграцією SCADA та хмари

Аналіз кібератак, спрямованих на хмарні системи SCADA, виявив чотири поширені вразливості:

- взаємозв'язок між системами SCADA та хмарними службами;
- використання спільної інфраструктури;
- присутність зловмисників інсайдерів;
- надійність безпеки протоколів SCADA.

Традиційні системи SCADA, розроблені як закриті системи без підключення до Інтернету, служать захисним механізмом. Однак міграція цих систем у хмару піддає їх складним мережевим середовищам, збільшуючи таким чином загрози безпеці, подібні до тих, з якими стикається будь-яка хмарна інфраструктура (Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019; Sajid, Abbas, & Saleem, 2016). У хмарних системах SCADA локальні пристрої можуть втратити зв'язок із віддаленими компонентами, що призведе до затримок у виробничих процесах, втрати даних і поширення помилок в інших компонентах системи (Bhamare та ін., 2020). Це пояснюється необхідністю підключення до хмарних центрів обробки даних, що є критичним аргументом проти впровадження хмарних обчислень (Yi, Mueller, Yu, & Chuan, 2017). Розгортання даних і програм у хмарі та доступ до них через Інтернет за своєю суттю підвищує вразливість системи до атак зловмисних користувачів (Nazir, Patel, & Patel, 2020).

На відміну від традиційних систем, компоненти хмарних систем SCADA не дотримуються єдиної системи безпеки, що призводить до непослідовної операційної продуктивності (Bhamare та ін., 2020). Це вимагає розгляду додаткових питань безпеки, включаючи відстеження хакерів, витік інформації, проблеми затримки та конфіденційності (Yadav, & Paul, 2021).

Таблиця 1. **Вразливість «Підключення між системою SCADA та хмарною службою» впливає на хмарні системи SCADA** (на основі статей за 2016—2024 рр.)

Вплив вразливості	Автор(и) публікації	Рік вразливості
Залежність від хмарного зв'язку робить систему SCADA більш вразливою до зовнішнього доступу	Sajid, Abbas, & Saleem	2016
Загрози безпеці зростають через необхідне підключення до публічної хмари	Yi, Mueller, Yu, & Chuan	2017
Підвищення ризиків, які потенційно можуть вплинути на безпеку хмарних систем SCADA	Stojanović, Boštjančić-Rakas, & Marković-Petrović	2019
Втрата з'єднання призводить до затримки процесів, втрати даних і проблем із конфіденційністю	Bhamare та ін.	2020
Зв'язок через публічну хмару наражає систему SCADA на потенційні кібератаки	Nazir, Patel, & Patel	2020
Покладення на хмарний зв'язок може наражати SCADA на атак типу «відмова в обслуговуванні» (DoS) і атак типу «людина посередині» (MITM)	Yadav, & Paul	2021

Спільне використання інфраструктури із зовнішніми неідентифікованими користувачами створює різні загрози для таких систем (Stojanović, Boštjančić-Rakas,

& Marković-Petrović, 2019). Зокрема, ризики пов'язані з можливістю спільного використання апаратної інфраструктури, як-от фізичних серверів, з іншими суб'єктами, такими як підприємства чи конкуренти. Ці об'єкти можуть використовувати методи впровадження команд/відповідей для системних атак. Це призводить до кількох наслідків, потенційно впливаючи на хмарні системи SCADA в їхніх критичних програмах реального часу (Nazir, Patel, & Patel, 2020). Функція багатокористування в хмарних технологіях створює значні ризики, особливо якщо гіпервізор або монітор віртуальної машини не мають надійного захисту. Вторгнення у віртуальні машини на одному гіпервізорі можуть спричинити зловмисну діяльність, порушуючи цілісність і конфіденційність даних критичної інфраструктури (Cerullo, Mazzeo, Papale, Sgaglione, & Cristaldi, 2016). Основні впливи вразливості спільної інфраструктури на хмарні системи SCADA підсумовано в табл. 2.

Таблиця 2. **Вразливість «Спільної інфраструктури» впливає на хмарні системи SCADA** (на основі статей за 2016—2024 рр.)

Вплив вразливості	Автор(и) публікації	Рік вразливості
Ризики безпеки виникають через функцію мультиорендування, притаманну хмарним технологіям	Cerullo, Mazzeo, Papale, Sgaglione, & Cristaldi	2016 рік
Спільне використання інфраструктури із зовнішніми сторонами наражає систему на ін'єкції команд/відповідей, включаючи атаки DoS і MITM	Stojanović, Boštjančić-Rakas, & Marković-Petrović	2019 рік
Хмарні постачальники не гарантують, що ресурси SCADA не будуть передаватись іншим підприємствам, що потенційно може призвести до загроз для системи	Nazir, Patel, & Patel	2020 рік

Зловмисні інсайдери, зазвичай, вважаються найсерйознішою загрозою для будь-якої системи, критичні системи, такі як системи SCADA, які контролюють промислові операції насамперед є метою таких зловмисників. Це можуть бути колишні співробітники, системні адміністратори або постачальники хмарних послуг із привілейованим доступом до системних ресурсів. Ці інсайдери створюють внутрішні вразливості системи безпеки (Sajid, Abbas, & Saleem, 2016; Cerullo, Mazzeo, Papale, Sgaglione, & Cristaldi, 2016). Різноманітні загрози безпеці, створені зловмисниками, включають несанкціонований доступ і контроль, порушення даних, крадіжку даних, маніпулювання даними та їх використання (Bhamare та ін., 2020).

Ці загрози безпеці можуть призвести до навмисних або ненавмисних помилок, потенційно завдаючи значної шкоди системі. Цей ризик підвищується, оскільки інсайдери володіють детальними знаннями про роботу системи (Nazir, Patel, & Patel, 2020). У контексті Інтернету речей (IoT) у хмарних системах SCADA співробітники, постачальники та підрядники часто підключаються до цих систем. Вони можуть мати дозвіл на доступ до мережевих датчиків або керування ними, дозволяючи їм додавати або оновлювати функції та отримувати доступ до виробничих даних і статистики. Спроби заблокувати або припинити ці форми авторизованого

доступу можуть призвести до завершення роботи хмарної системи SCADA всієї організації (Ulltveit-Moe та ін., 2016). У табл. 3 узагальнено основні впливи вразливості, спричинені фактором зловмисників у хмарних системах SCADA.

Таблиця 3. **Вразливість «зловмисних інсайдерів» впливає на хмарні системи SCADA** (на основі статей за 2016—2024 рр.)

Вплив вразливості	Автор(и) публікації	Рік вразливості
Зловмисні адміністратори хмарного постачальника (CP) або будь-який інший користувач із привілейованим доступом до ресурсів постійно загрожуватимуть системі	Cerullo, Mazzeo, Papale, Sgaglione, & Cristaldi	2016
Загрози, пов'язані із зовнішніми особами та постачальниками хмарних послуг	Sajid, Abbas, & Saleem	2016
Співробітники та постачальники, пов'язані з хмарою, можуть мати авторизований доступ до датчиків у мережі та/або контролю над ними, що потенційно може призвести до різноманітних ризиків безпеці	Cerullo, Mazzeo, Papale, Sgaglione, & Cristaldi	2016
Інші віддалені користувачі хмари зловживають недоліками системи	Bhamare та ін.	2020
Втрата доступу до ресурсів системи SCADA може бути спричинена як злими намірами співробітників КП, так і невинними помилками	Nazir, Patel, & Patel	2020

Іншим фактором, що сприяє вразливості хмарних систем SCADA до різноманітних загроз безпеці, є відсутність захисту в деяких традиційних протоколах зв'язку SCADA, таких як Modbus/TCP, серії 60870-5 Міжнародної електротехнічної комісії (IEC), IEC 61850 і DNP3 (Sajid, Abbas, & Saleem, 2016). Ці протоколи не підтримують механізми автентифікації та шифрування (Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019; Mesbah, Elsayed, Jurcut, & Azer, 2023) і страждають від відсутності елементів керування захистом (Yadav, & Paul, 2021). У результаті ці протоколи відкривають системні програми, що працюють у хмарі, і забезпечують зловмисникам легкий доступ до приватних облікових даних, таких як IP-адреси та імена користувачів, під час використання хмари. Крім того, неадекватна безпека в таких протоколах, як стандарт IEC 61850, який використовується для інтелектуальних електронних пристроїв на електричних підстанціях, використовує вразливі місця систем SCADA та створює ключові проблеми управління для мереж SCADA (Sajid, Abbas, & Saleem, 2016). У табл. 4 описано основний вплив цих вразливостей безпеки на хмарні системи SCADA.

Таблиця 4. **Вразливість «протоколів системи SCADA» впливає на хмарні системи SCADA** (на основі статей за 2016—2024 рр.)

Вплив вразливості	Автор(и) публікації	Рік вразливості
Системи SCADA використовують Modbus/TCP, IEC 61850 і DNP3 для автоматизації та керування. Однак ці протоколи не захищені та наражають операції керування та автоматизації на кібератаки	Sajid, Abbas, & Saleem	2016

Продовження таблиці 4

Спеціальні для SCADA протоколи прикладного рівня, такі як Modbus і DNP3, не підтримують елементи керування шифруванням і автентифікацією, що негативно впливає на безпеку хмарних систем SCADA	Stojanović, Boštjančić-Rakas, & Marković-Petrović	2019
Ризики безпеки в традиційній системі SCADA поширюються через відсутність засобів керування захистом у Modbus/TCP, IEC 40 та DNP3	Yadav, & Paul	2021

Кібератаки на хмарні системи SCADA розглядаються або широко (Bhamare та ін., 2020; Alakbarov, & Hashimov, 2023; Rashid, Gardiner, Green, & Craggs, 2019) або класифікують їх на основі конкретних критеріїв, таких як пасивний або активний, внутрішній або зовнішній (Maglaras та ін., 2018) та цілі атак (Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019; Pliatsios, Sarigiannidis, Lagkas, & Sarigiannidis, 2020; Ghosh, & Sampalli, 2019). Оскільки найпоширенішим критерієм класифікації багатьма дослідниками є ціль атаки або частина системи, яка зазнала атаки чи була використана, ми застосовуємо цей критерій у нашому опитуванні та розширюємо існуючу класифікацію на п'ять типів атак: апаратні, програмні, комунікаційні та протокольні, контроль процесу і внутрішні атаки на програмне забезпечення поділяються на категорії, пов'язані з ICS, на основі вразливостей або на хмару.

Апаратне забезпечення в хмарних системах SCADA взаємопов'язане з різноманітними глобальними компонентами та різними бібліотеками сторонніх розробників, що забезпечує складну взаємодію всередині систем. Основні апаратні елементи включають центр керування та контролери, такі як RTU, PLC та інтелектуальні електронні пристрої.

Центр управління збирає та аналізує дані з польових об'єктів, відображає ці дані на консолях HMI і діє на основі виявлених подій. Контрольні функції контролерів збирають дані та передають їх у хмару для зберігання та розповсюдження. Додаткові системні компоненти включають сервер MTU, сервери додатків, сервер Historian, інженерні робочі станції, сервер HMI та консолі, а також комунікаційні пристрої, такі як маршрутизатори, комутатори та модеми (Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019).

Загалом, постачальники систем SCADA знають про загрози безпеці апаратного забезпечення, такі як бекдор-атаки. Крім того, бездротові пристрої, які постачають дані традиційним системам SCADA, не мають надійного захисту через мінімальні вимоги до потужності, що є доступним вектором для системних вторгнень (Nazir, Patel, & Patel, 2020).

Апаратні атаки в хмарній інфраструктурі — це вразливі місця на апаратному рівні, включаючи ін'єкції троянських програм і порушення надійності та безпеки (McLaughlin та ін., 2016). Ці вразливості дозволяють несанкціоновану модифікацію мікропрограми, зворотне проєктування логіки через порти Joint Test Action Group і пошкодження друкованої плати через маніпулювання накопичувачами універсальної послідовної шини, що може змінити налаштування системи доменних імен (DNS), що призводить до перенаправлення зв'язку.

Ще одна складна апаратна атака, спрямована як на програмне, так і на апаратне забезпечення ICS, була описана в (Nazir, Patel, & Patel, 2020). У цій атаці використовується зловмисне програмне забезпечення Web Graphics Library для проникнення в апаратне забезпечення графічного процесора (GPU) через найменш привілейовані віддалені сторони, потенційно відкриваючи вміст із пам'яті GPU після робочих навантажень. Ця атака може поширюватися від центральної системи до інших пристроїв і використовуватися для ініціювання атак DoS, порушуючи роботу ICS.

Крім того, апаратне забезпечення системи SCADA може стати мішенню зловмисного програмного забезпечення, введеного в мікропрограму ПЛК, таким чином ставлячи під загрозу безпеку контролера. Крім того, несанкціонований доступ до фізичного розташування систем SCADA може призвести до суттєвих збоїв у роботі, включаючи втручання в налаштування критичних порогів (Irmak, & Erkek, 2018). Атаки на обладнання також можуть бути наслідком втрати живлення пристрою через перемикачі, навмисного пошкодження або фізичних атак на мережу керування (Chromik, Remke, & Haverkort, 2016).

Програмне системи SCADA охоплюють всі додатки, які використовуються для роботи систем SCADA додатки для керування обладнанням, збору інформації, процедур контролю та моніторингу, діагностики та обслуговування даних, а також середовища розробки клієнт/сервер і сторонніх розробників (Daneels, & Salter, 1999). Програмні атаки на системи SCADA викликають основне занепокоєння, ідентифікуються як кіберкінетичні атаки, які є складними та можуть загрожувати життю та завдати фізичної шкоди (Resul, & Gündüz, 2020). Ці кібератаки можна здійснити за допомогою різних методів, таких як ін'єкції зловмисного програмного забезпечення, ін'єкції команд/відповідей, фішинг, DoS-атаки, атаки ін'єкції SQL, атаки MITM та APT (Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019). У хмарних системах SCADA атаки на програмне забезпечення можна класифікувати як пов'язані з ICS, на основі вразливостей або специфічні для хмари.

Приклади загальних атак, які можуть вплинути на ICS, контрольовані системами SCADA, включаючи:

- атаки APT;
- атаки DDoS;
- пошкодження мережевих послуг голосу і даних;
- комбіновані кібер- та фізичні напади;
- атаки, ініційовані хактивістами;
- компрометації або збої в ланцюзі поставок (Bhamare та ін., 2020).

Кілька резонансних сценаріїв атак на ICS та критичну інфраструктуру, таких як інциденти MITM, ін'єкції запитів на керування, атаки на повторне відтворення на RTU та маніпуляції з керуванням контактами (Green, Krotofil, & Abbasi, 2017). Крім того, автори в (Rashid, Gardiner, Green, & Craggs, 2019) зазначили, що сприйняття помилки значно сприяли успіху цих атак. Ці помилки сприйняття пов'язані з чотирма вимірами: якістю системи, межами системи, спостережливістю та керованістю.

Існують різні програмні атаки, що впливають на критичну інфраструктуру систем SCADA, включно з вірусами-троянами, спалахами хробаків Stuxnet, хробаками Slammer, зловмисними програмами Flame, Dragonfly, DDoS і MITM (Tariq,

Asim, & Khan, 2019). Крім того, атаки на соціальному рівні, такі як соціальна інженерія, внутрішні загрози та фішингові схеми. Також описані кібератаки на системи SCADA електромереж, деталізуючи:

- пошкодження або втрату IT-активів через атаки, які маніпулюють системними даними;

- шкідливі дії, такі як зловживання IT-активами з навмисним втручанням в інформаційні системи (наприклад, DoS);

- підслуховування, перехоплення та викрадення, які сприяють несанкціонованому зв'язку із системними пристроями (наприклад, MITM) (Chromik, Remke, & Haverkort, 2016).

Програмні атаки — це вразливості на програмному рівні, починаючи від помилок кодування і закінчуючи неналежним впровадженням механізмів контролю доступу (Rashid, Gardiner, Green, & Craggs, 2019). З іншої боку, атаки на програмне забезпечення також описують як такі, що виникають через недоліки в дизайні та реалізації вихідного коду, включаючи такі проблеми, як переповнення буфера, впровадження SQL, міжсайтовий сценарій (XSS) і неадекватне керування виправленнями (Irmak, & Erkek, 2018).

Атаки на програмне забезпечення описують як використання зловмисниками слабких місць для отримання неавторизованого доступу до систем (Demertzis, & Iliadis, 2018). Наприклад, конкретні атаки, спрямовані на енергосистему SCADA, такі як введення команд віддаленого відключення, зміни налаштувань реле та атаки введення даних.

Атаки на програмне забезпечення розглядаються з різних точок зору, визнаючи їх викликами кібербезпеці та вразливими місцями, які потенційно можуть вплинути на системи SCADA, зокрема щодо виправлення та людського фактору (Cherdantseva та ін., 2016). Вони відзначили, що виправлення можуть ненавмисно створити нові вразливості або порушити роботу систем, особливо тих, які потребують безперервної роботи 24/7. Крім того, людський фактор може призвести до помилок, викликаючи ненавмисні атаки та соціальну інженерію, яка може призвести до навмисних внутрішніх і зовнішніх атак.

Загалом програмні атаки на хмарні системи SCADA передусім включають APT, порушення цілісності даних, атаки MITM, атаки відтворення та атаки DoS (Sajid, Abbas, & Saleem, 2016). Ці програмні атаки класифікуються на чотири категорії (Nechibvute, & Mafukidze, 2023):

- загрози доступності, що охоплюють віднімання пристрою, DDoS-атаки, крадіжки послуг, атаки на шляху та виснаження ресурсів вузла;

- загрози цілісності, пов'язані з неправильною конфігурацією, ін'єкцією зловмисного програмного забезпечення, ін'єкцією неправдивих даних, підробкою та маніпулюванням інформацією про маршрутизацію;

- загрози конфіденційності, які охоплюють крадіжку конфіденційної інформації, пасивний аналіз трафіку, розкриття статусу вузла та розголошення інформації про інфраструктуру;

- загрози автентифікації, включаючи ескалацію привілеїв, соціальну інженерію, неадекватний контроль доступу та уособлення вузла.

IIoT, що характеризується інтеграцією кібер- і фізичних систем, які полегшують обмін різними типами даних і конфіденційною інформацією, що дає змогу

інтелектуальним програмам і службам працювати точно в режимі реального часу, особливо вразливий до цих проблем безпеки програмного забезпечення в хмарних системах SCADA. Ці проблеми можуть призвести до помилок конфігурації або програмного забезпечення в операційних системах і програмному забезпеченні сторонніх виробників пристроїв IIoT, а також у каналах зв'язку. Вони також сприяють вразливості внутрішніх мережевих пристроїв, зовнішніх окремих постачальників послуг і постачальників хмарних послуг (Sajid, Abbas, & Saleem, 2016).

Атаки, які базуються на вразливостях нульового дня, найнебезпечніші, бо здатні уникати виявлення програмним забезпеченням для захисту від шкідливих програм (Rashid, Gardiner, Green, & Craggs, 2019). Ці атаки становлять значний ризик, оскільки мільйони пристроїв IoT можуть бути миттєво скомпрометовані, якщо в їхніх системах з'явиться невідома помилка програмного забезпечення. Загалом, інтеграція IoT у системи SCADA ускладнює забезпечення безпеки взаємопов'язаних пристроїв і може залучити деяких постачальників, продукти яких порушують протоколи безпеки зв'язку (Nechibvute, & Mafukidze, 2023).

Зручність доступу до хмарних систем з будь-якого місця в усьому світі також робить їх вразливими до атак зловмисників (Nazir, Patel, & Patel, 2020). Типи атак, такі як DoS, DDoS і MITM, стають все більш витонченими, уникаючи традиційних методів виявлення. Ба більше, стратегії захисту традиційних систем SCADA часто не підходять для боротьби з цими атаками.

Комунікаційні протоколи — це набори правил передачі та обміну даними через канали зв'язку. Протоколи зв'язку системи SCADA полегшують взаємодію між MTU і RTU (Yadav, & Paul, 2021). Як правило, протоколи системи SCADA не включають шифрування, що створює проблеми при розробці безпечних з'єднань і систем зв'язку (Nazir, Patel, & Patel, 2020).

Найбільш широко використовувані протоколи в системах SCADA включають Modbus і DNP3. Ці байт-орієнтовані протоколи використовуються в промислових системах для віддаленого виконання команд на керуючих пристроях. Однак при інтеграції в IP-мережі поширюється на всі машини в мережі. В Інтернеті ці протоколи стають сприйнятливими до кібератак і корупції через відсутність захисних заходів (Cai, Wang, & Yu, 2008).

Зловмисники, націлені на протоколи та комунікації системи SCADA, головним чином зосереджені на виявленні та використанні вразливостей у мережевих процесах (Demertzis, & Iliadis, 2018). У літературі ідентифікуються різні типи атак, наприклад атаки MITM через отруєння протоколу вирішення адрес, DNS отруєння, підробка мережевого протоколу часу, модифікація даних протоколу, використання правил протоколу (Rodofile, Radke, & Foo, 2019), а також на непотрібні порти та служби, вразливості каналів зв'язку та недоліки в протоколах зв'язку. Ці недоліки включають відсутність сертифікації, повноважень, шифрування та вразливість до атак DoS (Irmak, & Erkek, 2018).

Нарешті, існують атаки, розроблені спеціально для мережевих протоколів систем SCADA. До них належать атаки на протоколи мережевого рівня, націлені на такі елементи, як брандмауери, модеми, системи польових шин, системи зв'язку, маршрутизатори, віддалені точки доступу, а також протоколи та мережі керування (McLaughlin та ін., 2016). Інші атаки впливають на мережу системи SCADA в

цілому та спричиняють втрату доступності, цілісності та конфіденційності, а також проблеми відмови та відсутності автентифікації в протоколах розподіленої мережі (Ghosh, & Sampalli, 2019).

Атаки процесу керування на системи SCADA як вразливості рівня процесу (McLaughlin та ін., 2016). До них входить введення неправильної інформації для погіршення продуктивності керованого процесу, зміна змінних процесу виконання або логіки керування, а також пошкодження стану процесу. Отже, атаки на процес керування в системах SCADA, зазвичай, передбачають отримання зловмисниками контролю над цими системами (Demertzis, & Iliadis, 2018).

Різні приклади атак на процес управління на системи SCADA охоплюють атаки на модифікацію схемної логіки, функціональні атаки на схемну логіку, автоматизацію відтворення, викрадення з'єднання та атаки обману зворотного зв'язку (Rodofile, Radke, & Foo, 2019). Різні атаки, пов'язані з керуванням, на системи SCADA, такі як напади на контури зворотного зв'язку-контролю та фізичну інфраструктуру електромереж (Lin, Slagell, Kalbarczyk, Sauer, & Iyer, 2016).

Як наслідок, операції керування та безпеки в хмарних системах SCADA стикаються з такими проблемами, як затримки, втрата даних і скомпрометована надійність, безпека та конфіденційність (Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019).

Менеджери системи SCADA часто несуть відповідальність за втрату конфіденційності даних через обмежений контроль безпеки (Bhamare та ін., 2020). Інші користувачі хмари можуть використовувати вразливі місця в цих локальних засобах безпеки, що призведе до витоку даних. Деякі користувачі хмарних систем SCADA не визнають потребу в додаткових процесах і конфігураціях безпеки, демонструють відсутність відповідальності або не довіряють заходам безпеки, які пропонують постачальники хмарних послуг. Це призводить до значних інцидентів із загрозою кібербезпеці (Zhang, Luo, & Litvinov, 2021). Однією з головних загроз в IIoT є загроза від внутрішньої інформації, яка може бути реалізована співробітниками або постачальниками IIoT, уповноваженими на доступ або контроль мережевих датчиків (Ulltveit-Moe та ін., 2016). Інсайдери можуть робити навмисні чи ненавмисні помилки, потенційно завдаючи значної шкоди через знання системи. Крім того, працівники постачальника хмарних послуг, маючи повний доступ до даних, можуть зловживати ними для зловмисних цілей, таких як шпигунство або диверсія. Це також може статися через звичайну або ненавмисну помилку, що призводить до втрати доступу до ресурсів SCADA (Nazir, Patel, & Patel, 2020).

Відсутність ефективної автентифікації й авторизації користувачів (Tariq, Asim, & Khan, 2019) разом із підвищенням привілеїв, соціальною інженерією, неадекватним контролем доступу (Rubio, Alcaraz, Roman, & Lopez, 2019) та досвідчених інсайдерів, які можуть контролювати системи без підключених мереж або запроваджувати зловмисне програмне забезпечення (Zeng, & Zhou, 2018), також є основними загрозами безпеці та ризиками для хмарних систем SCADA.

На основі класифікації кібератак, очевидно, що три найпоширеніші та типові тактики, які потенційно можуть поставити під загрозу безпеку хмарної системи SCADA, це атаки DoS, MITM та APT. DoS-атаки спрямовані на те, щоб зробити послугу недоступною для законних користувачів. Це досягається шляхом наповнення цільової системи надмірним трафіком, доки вона не перестане відповідати

або не вийде з ладу, забороняючи таким чином доступ авторизованим користувачам. Ці атаки можна виконувати кількома способами, наприклад DoS або DDoS. Хоча DoS-атаки безпосередньо не завдають шкоди значним активам, вони можуть призвести до фінансових втрат і тимчасових витрат для компанії в періоди, коли її послуги та ресурси недоступні.

Зловмисники здійснюють атаки MITM, позиціонуючи себе в потоці зв'язку між користувачами хмари та хмарними програмами. Вони досягають цього за допомогою спуфінгу або сніфінгу. Під час спуфінгу зловмисник маскується під інших користувачів хмари, отримуючи доступ до хмарних систем SCADA. Це дає змогу їм обходити контроль безпеки або викрадати дані. Сніфінгові атаки передбачають перехоплення зловмисниками та моніторинг пакетів даних у хмарній системі SCADA. Це дає їм змогу отримувати конфіденційну інформацію, таку як паролі та облікові дані (Sajid, Abbas, & Saleem, 2016).

APT виникають, коли зловмисник або група зловмисників отримує несанкціонований доступ до мережі системи з наміром видобутку дуже конфіденційних даних. APT, зазвичай, використовують вразливості нульового дня, тобто діри в безпеці програмного забезпечення, про які постачальник не знає. Ці вразливості можливі після розробки системи або програмного забезпечення, і їх можна негайно використати без виявлення чи виправлення, що призводить до успішних атак (Bere, & Muyingi, 2015).

Ці три атаки є мережевими та представляють собою несанкціонований доступ до хмарних систем SCADA. Вони можуть призвести до системних збоїв і маніпулювання даними та повідомленнями в системі. Поширеною вразливістю в хмарних системах, яка призводить до вразливості атак DoS і MITM, є спільне використання інфраструктури. Для APT основною вразливістю є вразливість нульового дня.

У літературі пропонуються різні рішення безпеки, деякі з яких розроблені для хмарних обчислень загалом, а інші спеціально для хмарних систем SCADA. Існують розроблені рішення безпеки, адаптовані до хмарної інфраструктури, яка використовується в системах SCADA, охоплюючи публічні, приватні або гібридні моделі (Stojanović, Boštjančić-Rakas, & Marković-Petrović, 2019). Для публічних хмарних інфраструктур одне рішення передбачає використання технології push замість технології pull для переміщення даних у хмару. Цей підхід зменшує відкриті мережеві порти в мережі контролера, зменшуючи таким чином вплив системи SCADA на Інтернет. Інша стратегія зосереджена на захисті розташування хмарної інфраструктури та послуг, що надаються постачальником хмарних послуг, включаючи безпеку доступу користувачів, конфіденційність інформації, рівні контролю користувачів, керування файлами журналу для виявлення вторгнень і реагування на них, а також шифрування даних. На відміну від цього, основне рішення безпеки для приватної хмарної інфраструктури передбачає використання стратегії поглибленого захисту. Ця багаторівнева архітектура безпеки спрямована на мінімізацію впливу збою будь-якого окремого рівня та включає такі заходи, як розумний контроль доступу, брандмауери, системи виявлення та запобігання вторгненням, антивірусне програмне забезпечення тощо. Крім того, основним рекомендованим рішенням безпеки для гібридної хмарної інфраструктури є використання безпечних віртуальних приватних мереж для керування інфраструктурою.

Існує низка оптимальних методів захисту хмарних систем SCADA (Sajid, Abbas, & Saleem, 2016). До них належать розділення мереж, аналіз журналів, аналіз мережевого трафіку, використання інструментів для регулярного виявлення зловмисних дій, проведення стандартного тестування вразливостей, впровадження постійного моніторингу та аналізу, виконання моніторингу цілісності файлів, ретельний аналіз дампів пам'яті, послідовне оновлення та виправлення, а також використання проксі-сервера.

Також підхід базується на шифруванні на основі атрибутів політики зашифрованого тексту (CP-ABE), щоб забезпечити детальний контроль доступу до даних, що зберігаються в хмарі, враховуючи як статичні, так і динамічні атрибути користувача (Routray, & Bera, 2023). Структура безпеки розроблена для запобігання несанкціонованому доступу до даних, витоку даних і приховуванню політики доступу для забезпечення конфіденційності даних. Цей підхід використовує туманні сервери для перевірки динамічних атрибутів користувачів і звільнення від кінцевих користувачів обчислювальних завдань, що, у свою чергу, зменшує витрати на обчислення, роблячи систему більш масштабованою та ефективною.

Іншою технікою є приманки SCADA, зокрема приманки з низьким рівнем взаємодії під назвою Conpot, для виявлення потенційних зловмисних дій у мережах SCADA (Mesbah, Elsayed, Jurcut, & Azer, 2023). Крім сегментації мережі, контролю доступу та систем виявлення вторгнень, організації можуть використовувати приманки для усунення ризиків атак операційних технологій (OT) (наприклад, PLC, RTU, HMI тощо) у хмарних системах та системах на основі IoT. Використання приманок або систем-приманок, призначених для відволікання зловмисників від реальних активів, дає змогу збирати цінну інформацію про шаблони атак. Аналіз даних honeypot допомагає зрозуміти динаміку атак OT і покращити механізми безпеки. Зокрема, приманки SCADA дають змогу адміністраторам безпеки виявляти вразливі місця системи шляхом імітації цілей зловмисника в контрольованому середовищі та моніторингу поведінки зловмисників. Це може виявити нові техніки та методи атак і покращити безпеку системи SCADA шляхом виправлення вразливостей і впровадження більш сильних заходів безпеки. Однак honeypot (пастки) слід розгортати безпечно, щоб мінімізувати потенційні загрози привернути більше уваги зловмисників.

Основні типи IDS (хмарні системи виявлення вторгнень) та IPS (системи запобігання вторгненням) для хмарних обчислень включають систему виявлення вторгнень на основі хосту (HIDS)/систему запобігання вторгнень на основі хосту (HIPS) і систему виявлення вторгнень на основі мережі (NIDS)/систему запобігання вторгненню в мережу (NIPS) (Alam, Shuaib, & Samad, 2019). Функція HIDS/HIPS шляхом моніторингу, аналізу та запобігання аномаліям у даних, зібраних з хост-машин. Ці дані надходять із файлових систем, баз даних і аналізів мережевих обчислювальних систем. При виявленні аномалій для профілактики спрацьовує сигналізація. NIDS/NIPS, навпаки, відстежує та виявляє зловмисний трафік у мережі, перевіряючи всі мережеві пакети на наявність шкідливих шаблонів. У разі атаки NIDS/NIPS сповіщає адміністраторів або блокує джерело IP від доступу до мережі, залежно від серйозності атаки.

Як обговорювалося раніше, атаки DoS, MITM і APT в основному спрямовані на мережеву інфраструктуру хмарних систем SCADA. Таким чином, NIDS/NIPS,

мабуть, є більш ефективним у захисті цих систем від різних кібератак порівняно з методами HIDS/HIPS.

Висновки

У цьому дослідженні розглядалися вразливості та кібератаки, що впливають на безпеку хмарних систем SCADA. Було визначено чотири основні області вразливості: зв'язок між системами SCADA та хмарними службами, спільна інфраструктура, присутність зловмисників інсайдерів і надійність безпеки протоколів SCADA. Крім того, це дослідження класифікувало кібератаки на п'ять груп: апаратне забезпечення, програмне забезпечення, атаки, пов'язані з зв'язком і протоколом, атаки на процес керування та атаки зсередини. Було виявлено, що DoS, MITM і APT становлять найбільшу загрозу для цих систем через їхню залежність від спільних інфраструктур, промислових операцій у реальному часі та високої доступності. Також розглянуто кілька рішень безпеки для пом'якшення цих загроз. Оскільки найпоширеніші атаки є мережевими (такі як DoS, MITM і APT), це дослідження підтверджує, що мережеві IDS/IPS (NIDS/NIPS) є ефективними заходами безпеки для виявлення та запобігання кібератакам, захищаючи таким чином хмару системи SCADA.

У той час, як наше дослідження охоплювало різні вразливості, атаки та механізми безпеки, різноманітні загрози й атаки залишаються непокритими поточними рішеннями, такими як складне шкідливе програмне забезпечення (наприклад, програми-вимагачі та шпигунські програми), які можуть адаптуватися та видозмінюватися, щоб уникнути виявлення, а також недостатній рівень безпеки (наприклад, паролі за замовчуванням або незашифрований зв'язок) у пристроях IoT, що робить їх м'якими мішенями для зловмисників. Крім того, залежність від постачальників хмарних технологій для забезпечення безпеки піддає системи SCADA ризику, якщо постачальники не впроваджують суворих заходів безпеки або якщо вони самі скомпрометовані. Оскільки хмарні системи SCADA часто покладаються на компоненти та послуги від кількох постачальників, вони сприйнятливі до атак на ланцюг поставок (наприклад, скомпрометовані оновлення програмного забезпечення). Складні атаки на ланцюжок поставок, що відбуваються нагорі, можуть вплинути на системи SCADA, і такі ризики не завжди можуть враховуватися в поточних моделях безпеки. Озброєні ПЛК становлять значну загрозу в хмарних системах, де зловмисне програмне забезпечення може бути встановлено в ПЛК, щоб змінити їх функціонування або використовувати їх як точки входу для проникнення в системи SCADA.

Однією з найбільш значних нових загроз для хмарних систем є концепція змагального штучного інтелекту (AI) (Anthi, Williams, Rhode, Burnap, & Wedgbury, 2021), де моделями машинного навчання маніпулюють або для того, щоб ввести в оману системи безпеки, або для здійснення атак на системи SCADA. Наприклад, група APT може використовувати модель машинного навчання для аналізу шаблонів у мережевому трафіку системи SCADA або визначення регулярних періодів обслуговування та інтервалів передачі даних. Цю модель можна навчити імітувати звичайні шаблони мережевого трафіку, генерувати трафік, який поєднується з регулярними даними технічного обслуговування, і уникати виявлення під час відображення мережі. Моделі машинного навчання також можуть вивчати робочі

шаблони системи SCADA, включаючи балансування навантаження, цикли перемикання підстанції та налаштування трансформатора, таким чином отримуючи контроль над декількома ПЛК і непомітно змінюючи навантаження трансформатора для створення дисбалансу. Зловмисники планують, щоб ці зміни відбувалися одночасно в години пікового використання, щоб максимізувати вплив. Раптова несподівана зміна навантаження може спричинити каскадний збій у мережі, що призведе до втрати електроенергії. У таких випадках інженерам може бути важко визначити причину збоїв, що призведе до подовження часу відновлення. Підхід, керований штучним інтелектом, не тільки забезпечує початкове проникнення, але й дає змогу зловмисникам навчитися й адаптуватися до поведінки системи, що робить атаку дуже ефективною та складною для пом'якшення або виявлення засобами безпеки.

Щоб усунути раніше виявлені загрози та атаки, організаціям, які впроваджують інфраструктуру хмарної системи SCADA, слід розглянути різні важливі кроки. Наприклад:

- впровадження систем моніторингу безпеки в реальному часі, які можуть адаптуватися до нових загроз, що розвиваються, що, у свою чергу, може зменшити вікно можливостей для зловмисників;

- наявність надійного плану реагування на інциденти, який можна швидко й ефективно запровадити у разі порушення безпеки;

- виконання регулярних комплексних перевірок безпеки, включаючи сканування вразливостей і тестування на проникнення, щоб виявити потенційні прогалини в безпеці;

- розробка надійних інфраструктур безпеки для пристроїв Інтернету речей, інтегрованих у системи SCADA, щоб гарантувати, що ці пристрої не стануть точками входу для зловмисників.

- підвищення безпеки ланцюга постачання завдяки тісній співпраці з постачальниками та партнерами, щоб переконатися, що вони дотримуються високих стандартів безпеки;

- підвищення обізнаності та навчання серед працівників для запобігання порушенням безпеки через людські помилки або внутрішні загрози, а також

- участь у співпраці для обміну інформацією про загрози, що може допомогти у швидшій ідентифікації та реагуванні на нові загрози.

Крім того, використання штучного інтелекту та алгоритмів машинного навчання може передбачити атаки на системи SCADA та покращити виявлення складних і раніше невідомих шаблонів атак. Ці алгоритми також можуть виявляти аномальну поведінку, яка може вказувати на те, що ПЛК було зламано. Для захисту від атак, керованих штучним інтелектом, і ПЛК із використанням зброї, системні адміністратори та групи безпеки повинні розглянути такі методи, як поєднання перевірок цілісності апаратного та програмного забезпечення, аналіз поведінки, керований штучним інтелектом, і створення безпечного життєвого циклу розробки для програмного забезпечення ПЛК. Адаптація нормативних актів і стандартів для обов'язкових практик безпечного кодування та журналів аудиту ШІ має вирішальне значення для запобігання зловмисним діям ШІ. Також важливо регулярно виправляти відомі та потенційні вразливості, особливо в хмарному середовищі, де загрози можуть швидко зростати.

Безпека хмарних систем SCADA є надзвичайно важливим питанням, яке потребує більш ретельного дослідження. Вирішення проблем безпеки цих систем є життєво важливим для запобігання майбутнім інцидентам і катастрофічним подіям. Майбутні дослідження мають вивчити кілька невивчених типів загроз. Це включає квантові атаки, коли традиційні методи шифрування можуть застаріти. Дослідники повинні присвятити зусилля квантово-стійким криптографічним методам, щоб захистити хмарні системи SCADA від майбутніх загроз. Окрім квантових загроз, безпека ланцюга постачання потребує уваги дослідників, включаючи розробку платформ для оцінки стану безпеки сторонніх постачальників і механізмів для виявлення скомпрометованих програмних або апаратних компонентів. Незважаючи на технологічний прогрес, людський фактор і внутрішні загрози залишаються критично вразливими місцями. Дослідження складного контролю доступу, поведінкової аналітики та механізмів виявлення внутрішніх загроз можуть запропонувати значні покращення безпеки. У майбутніх дослідженнях слід також наголошувати на розширеній оцінці ризиків безпеки та важливості проведення відповідних тестових стендів для перевірки рішень безпеки для цих систем. Крім того, впровадження розширених заходів безпеки на основі штучного інтелекту та розгляд безпеки як невід'ємного компонента проектування системи є критично важливими для хмарних систем SCADA. Зосереджуючись на цих областях, майбутні дослідження можуть розглянути мінливий ландшафт загроз, з якими стикаються хмарні системи SCADA, і сприяти розробці більш стійких рішень безпеки.

Література

Alakbarov, R., & Hashimov, M. (2023). *Development of Security Mechanisms in Cloud Based SCADA Systems.* In Proceedings of the 2023 5th International Conference on Problems of Cybernetics and Informatics. doi:10.1109/pci60110.2023.10325946.

Alam, S., Shuaib, M., & Samad, A. (2019). *A collaborative study of intrusion detection and prevention techniques in cloud computing,* In Proceedings of the International Conference on Innovative Computing and Communications. doi:10.1007/978-981-13-2324-9_23.

Anthi, E., Williams, L., Rhode, M., Burnap, P., & Wedgbury, A. (2021). Adversarial attacks on machine learning cybersecurity defences in industrial control systems. *Journal Information Security Application,* 58, 102717.

Bere, M., & Muyingi, H. (2015). *Initial investigation of industrial control system (ICS) security using artificial immune system (AIS).* In Proceedings of the 2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC). doi:10.1109/etncc.2015.7184812.

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *Computer Security,* 89, 101677.

Buyya, R., Yeo, C. S., & Venugopal, S. (2008). *Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities.* In Proceedings of the 2008 10th IEEE International Conference on High Performance Computing and Communications. Dalian: IEEE.

Byers, C. (2018). *Fog Computing for Industrial Automation.* Взято з https://www.controleng.com/articles/fog-computing-for-industrial-automation/.

Cai, N., Wang, J., & Yu, X. (2008). *SCADA system security: Complexity, history and new developments.* In Proceedings of the 2008 6th IEEE International Conference on Industrial Informatics. doi:10.1109/indin.2008.4618165.

Cerullo, G., Mazzeo, G., Papale, G., Sgaglione, L., & Cristaldi, R. (2016). *A Secure Cloud-Based SCADA Application: The Use Case of a Water Supply Network.* In Proceedings of the International Conference on New Trends in Intelligent Software Methodology Tools and Techniques. Larnaca: SoMeT 16.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computer security*, 56, 1—27.

Chromik, J. J., Remke, A., & Haverkort, B. R. (2016). *Improving SCADA security of a local process with a power grid model*. In Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research. doi:10.14236/ewic/ics2016.13.

Church, P., Mueller, H., Ryan, C., Gogouvitis, S. V., Goscinski, A., Haitof, H., & Tari, Z. (2015). *Moving SCADA systems to IaaS clouds*. In Proceedings of the 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity). doi:10.1109/smartcity.2015.186.

Church, P., Mueller, H., Ryan, C., Gogouvitis, S. V., Goscinski, A., Haitof, H., & Tari, Z. (2017). *In Handbook of Big Data Technologies. SCADA systems in the Cloud.* Berlin: Springer.

Combs, L. (2011). *Cloud computing for SCADA. Control Engineering.* Взято з https://www.controleng.com/articles/cloud-computing-for-scada/.

Daneels, A., & Salter, W. (1999). *What is SCADA?*. In Proceedings of the International Conference on Accelerator and Large Experimental Physics Control Systems. Trieste: Conf. Proc. C.

Davis, C., Tate, J., Okhravi, H., Grier, C., Overbye, T., & Nicol, D. (2006). *SCADA cyber security testbed development*. In Proceedings of the 2006 38th North American Power Symposium. doi:10.1109/naps.2006.359615.

Demertzis, K., & Iliadis, L. (2018). *Modern Discrete Mathematics and Analysis: A computational intelligence system identifying cyber-attacks on smart energy grids* (1st ed). Berlin: Springer.

El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. *Computer and Electrical Engineering*, 67, 469—482.

Ghosh, S., & Sampalli, S. (2019). A survey of security in SCADA networks: Current issues and future challenges. *IEEE Access*, 7, 135812—135831.

Green, B., Krotofil, M., & Abbasi, A. (2017). *On the significance of process comprehension for conducting targeted ICS attacks*. In Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy. doi: 10.1145/3140241.3140254.

Howard, P. (2015). *Checklist for SCADA Systems in the Cloud.* Взято з https://www.route-fifty.com/infrastructure/2015/06/a-security-checklist-for-scada-systems-in-the-cloud/287164/.

Irmak, E., & Erkek, I. (2018). *An overview of cyber-attack vectors on SCADA systems*, In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS). doi:10.1109/isdfs.2018.8355379.

Lin, H., Slagell, A., Kalbarczyk, Z. T., Sauer, P. W., & Iyer, R. K. (2016). Runtime semantic security analysis to detect and mitigate control- related attacks in power grids. *IEEE Transactions on Smart Grid*, 9, 163—178.

Maglaras, L., Ferrag, M., Derhab, A., Mukherjee, M., Janicke, H., & Rallis, S. (2018). Threats, countermeasures and attribution of cyber attacks on critical infrastructures. *EAI Endorsed Transactions on Security and Safety*. doi:10.4108/eai.15-10-2018.155856.

McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, 104, 1039—1057.

Mesbah, M., Elsayed, M. S., Jurcut, A. D., & Azer, M. (2023). Analysis of ICS and SCADA Systems Attacks Using Honeypots. *Future Internet*, 15, 241. doi:10.3390/fi15070241.

Molle, M., Raithel, U., Kraemer, D., Graß, N., Söllner, M., & Aßmuth, A. (2019). *Security of cloud services with low-performance devices in critical infrastructures,* In Proceedings of the Cloud Computing 2019, The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization. doi:10.48550/arXiv.2405.11368.

Morsey, C. (2017). *Supervisory Control and Data Acquisition (SCADA) Systems and Cyber-Security: Best Practices to Secure Critical Infrastructure.* (Dissertation, D. Sc.). Robert Morris University, Pittsburgh.

Mushtaq, M. F., Akram, U., Khan, I., Khan, S. N., Shahzad, A., & Ullah, A. (2017). Cloud computing environment and security challenges: A review. *International Journal of Advanced Computer Science and Applications*, 8, 183—195.

Nazir, S., Patel, S., & Patel, D. (2020). Cloud-based autonomic computing framework for securing SCADA systems. *In Innovations, Algorithms, and Applications in Cognitive Informatics and Natural Intelligence*, 276—297. doi:10.4018/978-1-7998-3038-2.ch013.

Nechibvute, A., & Mafukidze, H. (2023). Integration of scada and industrial iot: Opportunities and challenges. *IETE Technical Review*, 1—14. doi:10.1080/02564602.2023.2246426.

Nugent, E. (2017). How Cloud and Fog Computing will Advance SCADA Systems. *Manufacturing Automation*, 32, 22—24.

Pliatsios, D., Sarigiannidis, P., Lagkas, T., & Sarigiannidis, A. G. (2020). A survey on SCADA systems: Secure protocols, incidents, threats and tactics. *IEEE Communications Surveys & Tutorials*, 22, 1942—1976.

Rakas, S. V. B., Stojanović, M. D., & Marković-Petrović, J. D. (2020). A review of research work on network-based scada intrusion detection systems. *IEEE Access*, 8, 93083—93108.

Rashid, A., Gardiner, J., Green, B., & Craggs, B. (2019). *Everything is awesome! Or is it? Cyber security risks in critical infrastructure.* In Proceedings of the International Conference on Critical Information Infrastructures Security, 3—17. doi:10.1007/978-3-030-37670-3_1.

Resul, D., & Gündüz, M. Z. (2020). Analysis of cyber-attacks in IoT-based critical infrastructures. *International Journal of Information Security*, 8, 122—133.

Rodofile, N. R., Radke, K., & Foo, E. (2019). Extending the cyber-attack landscape for SCADA-based critical infrastructure. *International Journal of Critical Infrastructure Protection*, 25, 14—35.

Routray, K., & Bera, P. (2023). *Context-Aware Attribute Based Access Control for Cloud-based SCADA Systems.* In Proceedings of the 1st Workshop on Enhanced Network Techniques and Technologies for the Industrial IoT to Cloud Continuum, 35—40. doi:10.1145/3609389.3610569.

Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. *Computer security*, 87, 101561.

Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access*, 4, 1375—1384.

Saliieva O., & Yaremchuk, Yu. (2020). Cognitive model for studying the level of protection of a critical infrastructure object. *Ukrainian Scientific Journal of Information Security*, 26(2), 64—73.

Stojanović, M. D., Boštjančić-Rakas, S. V., & Marković-Petrović, J. D. (2019). SCADA systems in the cloud and fog environments: Migration scenarios and security issues. *Facta Universitatis Series Electronics and Energetics*, 32(3), 345—358. doi:10.2298/fuee1903345s.

Tariq, N., Asim, M., & Khan, F. A. (2019). Securing SCADA-based critical infrastructures: Challenges and open issues. *Procedia Computer Science*, 155, 612—617.

Ulltveit-Moe, N., Nergaard, H., Erdödi, L., Gjøsæter, T., Kolstad, E., & Berg, P. (2016). *Secure information sharing in an industrial Internet of Things*. doi:10.48550/arXiv.1601.04301.

Wilhoit, K. (2013). *SCADA in the Cloud.* Trend Micro: Cupertino. 5 c.

Yadav, G., & Paul, K. (2021). Architecture and security of SCADA systems: A review. *International Journal of Critical Infrastructure Protection*, 34, 100433.

Yi, M., Mueller, H., Yu, L., & Chuan, J. (2017). *Benchmarking cloud-based SCADA system.* In Proceedings of the 2017 IEEE International Conference on Cloud Computing Technology and Science (Cloud Com), 122—129. doi:10.1109/cloudcom.2017.25.

Zeng, P., & Zhou, P. (2018). Intrusion detection in scada system: A survey. *In Intelligent Computing and Internet of Things*, 342—351. doi:10.1007/978-981-13-2384-3_32.

Zhang, S., Luo, X., & Litvinov, E. (2021). Serverless computing for cloud-based power grid emergency generation dispatch. *International Journal Electrical Power Energy Systems*, 124, 106366.