policies across the entire distributed infrastructure. Data from various cloud platforms, event logs, and network traffic is consolidated and normalized. Moreover, integrating API gateways and service meshes into this architecture allows for granular policy enforcement, ensuring secure machine-to-machine (M2M) communication across different cloud boundaries. This centralized visibility also simplifies compliance with stringent regulatory frameworks, such as GDPR or HIPAA, by providing a unified trail of access logs.

Machine learning and artificial intelligence algorithms play a crucial role in developing adaptive policies by enabling User and Entity Behavior Analytics (UEBA). Models detect hidden correlations and anomalies that may indicate credential compromise or insider abuse attempts, automatically adjusting the user's "trust score" in real time. By utilizing both supervised learning for known threat signatures and unsupervised learning for novel anomaly detection, these intelligent systems can proactively isolate compromised accounts before significant data exfiltration occurs.

Thus, the development and implementation of adaptive access control policies are critical for protecting modern distributed information systems. The integration of dynamic context assessment, attribute-based access models, and behavior analytics allows for the creation of a resilient architecture that effectively counters cyber threats in complex multi-cloud ecosystems.

References

1. National Institute of Standards and Technology. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg: NIST, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207.

2. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing. URL: https://cloudsecurityalliance.org/ (accessed: 14.10.2026).

3. National Institute of Standards and Technology. Attribute Based Access Control (ABAC) Definition and Considerations. NIST SP 800-162. Gaithersburg: NIST, 2014. DOI: https://doi.org/10.6028/NIST.SP.800-162.

4. Development and standardization of information security policies in cloud environments: current state and prospects.

УДК 004.056:681.518

КІБЕРЗАХИСТ СИСТЕМ SCADA: АКТУАЛЬНІ ЗАГРОЗИ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Євген Губницький

Миколаївський національний аграрний університет, м. Миколаїв, Україна

Науковий керівник: Л. О. Борян,
старший викладач Миколаївський національний аграрний університет

Інтенсивна цифровізація виробничих процесів, індустріальна автоматизація та впровадження концепції Індустрії 4.0 зумовили глибоку інтеграцію інформаційних технологій (IT) та операційних технологій (OT). Центральне місце в цій екосистемі займають диспетчерські системи управління та збору даних Supervisory Control and Data Acquisition (SCADA). Вони забезпечують безперервний моніторинг, збір телеметричної інформації та керування складними технологічними об'єктами в реальному часі: від енергетичних мереж і гідроелектростанцій до агропромислових комплексів, систем зрошення та переробки [1]. Однак історично архітектура SCADA-систем розроблялася з розрахунку на ізольованість і фізичну безпеку, а не на протидію цілеспрямованим кібератакам із боку злочинних угруповань чи держав-агресорів [4]. Перехід до використання стандартних мережевих протоколів (Modbus, Profibus, DNP3 поверх TCP/IP), підключення промислових мереж до глобальної мережі Інтернет та використання хмарних сховищ перетворили критично важливі об'єкти країни на вразливі мішені. Відтак, забезпечення надійного кіберзахисту SCADA є питанням безпеки й життєдіяльності держави.

Типова архітектура SCADA складається з кількох рівнів: польовий рівень (Field Level) - датчики, виконавчі механізми, контролери (PLC – Programmable Logic Controllers), які безпосередньо взаємодіють із технологічним середовищем; рівень управління (Control Level) - станції операторів, локальні сервери збору даних, людино-машинний інтерфейс (HMI); рівень корпоративної мережі (Enterprise Level) - системи планування ресурсів (ERP), бази даних підприємства та адміністративні робочі місця. Злиття OT та IT-мереж розриває традиційний захисний периметр («повітряний зазор» - *air-gap*) [4]. Сучасні критичні системи управління ускладнені такими факторами як використання застарілого програмного забезпечення та операційних систем на рівні робочих станцій диспетчерів, які часто не підтримують актуальні патчі безпеки через ризики порушення безперебійності технологічного циклу, слабкий або відсутній захист протоколів зв'язку - більшість традиційних промислових протоколів не передбачають вбудованого шифрування та ідентифікації повідомлень, що дозволяє зловмисникам здійснювати атаки типу «людина посередині» (MitM) або перехоплювати керуючі команди [2].

Кібератаки на промислові об'єкти - це одна з найбільших загроз для національної та економічної безпеки. На відміну від IT-сектор, де зловмисники полюють на дані, цільова атака на промисловість є руйнуванням фізичних процесів, зупинкою виробництва та створенням техногенних катастроф [1]. Зловмисники зазвичай використовують слабкі місця на стику корпоративної (IT) та технологічної мереж, компрометація через корпоративну мережу (IT-до-OT**)** - найпоширеніший шлях, хакери зламують офісну мережу підприємства (наприклад, через фішинг), а потім проникають усередину технологічного контуру через недостатньо ізольовані мережеві мости, атаки із ланцюжка постачань (Supply Chain Attacks) тобто злам підрядників, які мають легітимний віддалений доступ для обслуговування промислового обладнання, або впровадження шкідливого коду безпосередньо в оновлення програмного забезпечення (ПЗ) від виробників, вразливості віддаленого доступу (RDP/VPN) - використання слабких або викрадених облікових даних співробітників чи інженерів, які працюють дистанційно, свідомі дії підкуплених чи ображених співробітників або випадкова помилка персоналу (наприклад, підключення зараженої флешки безпосередньо до робочої станції оператора SCADA, недостатня кібергігієна обслуговуючого персоналу, використання неперевірених дискових носіїв (USB-накопичувачів), слабкі паролі доступу до інженерних станцій. Ключові наслідки кібератак промислових кібератак поділяються на кілька категорій таких як фізичні руйнування та екологія - пошкодження дорогого обладнания (турбіни, генератори, печі), спровоковані вибухи, пожежі, витоки хімікатів чи радіації, економічні збитки - простій виробництва, кожна година зупинки конвеєра коштує мільйони, величезні витрати на відновлення інфраструктури та аудит, травмування або загибель персоналу на виробництві, загроза для цивільного населення, наприклад, через отруєння води або відключення тепла/світла, втрата контрактів та довіри інвесторів, штрафи від державних регуляторів за порушення норм безпеки, дестабілізація критичної інфраструктури (енерготекери, транспорт, водопостачання) під час міждержавних конфліктів [1].

Основними векторами та класифікаціями атак є цілеспрямовані атаки типу APT (Advanced Persistent Threat)**,** тобто зловмисники роками закріплюються в корпоративній мережі підприємства, поступово проникаючи через компрометацію суміжних сервісів (підрядників, підрядників) до ізольованого сегмента OT, також шкідливе програмне забезпечення-вимагачі (Ransomware), що займається шифруванням баз даних або робочих станцій і паралізує процес моніторингу, змушуючи операторів переходити на ручне аварійне управління, фальсифікація даних телеметрії методом введення хибних показників датчиків і змушує автоматику або операторів ухвалювати помилкові рішення, що може призвести до аварій техногенного характеру.

З математичної точки зору ризик кібератаки R можна описати класичною функцією:

$$R = P \times V \times I,$$

де P - ймовірність реалізації загрози (активність зловмисників), V - вразливість системи (слабкі місця архітектури), а I - масштаби потенційних збитків (екологічні, економічні та соціальні наслідки). Оскільки показник наслідків для SCADA-систем є надзвичайно високим, навіть мінімальна ймовірність P вимагає максимального зниження системних вразливостей I [1].

Для захисту промислових об'єктів (ICS/SCADA) розроблено суворі міжнародні інструкції [3] такі як ISA/IEC 62443 - головний глобальний стандарт, що визначає вимоги до кібербезпеки технологічних систем на всіх етапах (від проєктування до експлуатації). Він пропонує концепцію «захисту в глибину», NIST SP 800-82 - Посібник із безпеки промислових систем керування від Національного інституту стандартів і технологій США [3], директива NIS 2 (ЄС) - законодавство, що зобов'язує підприємства критичної інфраструктури впроваджувати жорсткі заходи кіберзахисту та звітувати про інциденти.

Для ефективного протистояння сучасним кіберазагам компанії повинні базуватися на принципі «Нульової довіри» (Zero Trust Architecture) та ешелонованого захисту, архітектурного та мережевого методу захисту - мережева сегментація та брандмауери нового покоління (NGFW), тобто сувора відокремлена корпоративної мережі від технологічного сегмента за допомогою демілітаризованих зон (DMZ) та промислових міжмережевих екранів, що фільтрують трафік на рівні прикладних протоколів OT, системи виявлення та запобігання вторгненням (IDS/IPS) - впровадження спеціалізованих рішень глибокого аналізу пакетів (DPI - Deep Packet Inspection), здатних розпізнавати аномалії в промислових протоколах (наприклад, несанкціоновані команди запису регістрів PLC [4]), технологія Data Diode (односпрямовані шлюзи) - апаратні пристрої, які дозволяють передавати дані лише в один бік (наприклад, з мережі до корпоративну мережу для аналітики).

Передавати команду назад у SCADA через такий пристрій фізично неможливо. Шифрування промислових протоколів - це перехід на захищені версії протоколів (наприклад, OPC UA Security, Modbus Security, IEC 62353), які примушують шифрування трафіку та автентифікацію пристроїв, що унеможливлює підміну команди (Spoofing)) [2]. Використання технологічного моніторингу та зниження загроз, у SCADA-мережах не можна використовувати агресивні сканери вузлів. Тому використовуються пасивні методи [2] - промислові системи виявлення вторгнень (Industrial IDS): системи (наприклад, Cisco Cyber Vision, Microsoft Defender for IoT), які підключаються до дзеркального порту (SPAN) комутатора. Вони пасивно слухають трафік, будують карту мережі, створюють базову лінію нормальної поведінки (Baseline) та сигналізують про будь-які аномалії чи появу нових пристроїв, виконується збір та кореляція логів з SCADA-серверів, інженерних станцій, шлюзів та комутаторів в єдиний центр керування безпекою (SOC).

Замість класичних антивірусів, які потребують щоденних оновлень баз, використовують блокування за білими списками, на комп'ютері дозволяється запуск лише конкретного ПЗ для SCADA, будь-який інший файл (навіть принесений на флешці) просто не запуститься, контроль периферійних пристроїв (USB Lockdown) - повне апаратне або програмне блокування USB-портів на робочих станціях операторів для запобігання випадковому чи навмисному зараженню, управління патчами (Patch Management за регламентом) - оновлення ОС та ПЗ SCADA проводяться тільки після ретельного тестування на полігонах (Staging середовище) та під час планових технологічних зупинок підприємства.

Діофакторна автентифікація (2FA/MFA) обов'язкова для будь-якого віддаленого підключення підрядників або інженерів до промислової мережі через VPN, управління привілейованим доступом (PAM) - контроль дій інженерів та розробників. Усі сесії віддаленого доступу записуються на відео, а права на зміну логіки PLC називаються тимчасовими (Just-in-Time access). Можна порівняти засоби захисту, які використовуються: Industrial Firewall – захищає периметр мережі, перевага у фільтруванні команд на рівні промислових протоколів, вимагає глибокого технологічного розуміння, Data Diode – захищає найкритичніші сегменти (ядро), перевага у 100% апаратному захисті від зловмисних кібератак, повністю блокує зворотний рух (сторонній рух), Industrial IDS – захищає усю мережу OT, перевага у безпечному пасивному моніторингу без впливу на PLC, потребує налаштування для виключення хибних тривог, Application Whitelisting - захищає HMI та інженерні станції, перевага у захисті від невідомих вірусів (Zero-day), блокує встановлення будь-якого ПЗ без білого списку.

Виходячи з вищевказаного можна зробити висновок, що кіберзахист систем SCADA є критично важливим елементом забезпечення сталого функціонування об'єктів критичної інфраструктури,

енергетики та промисловості [1]. Еволюція кіберзагрози вимагає відмови від застарілих підходів щодо ізольованості мережевих мереж і переходу до комплексних систем активного захисту на базі принципів Zero Trust, глибокого моніторингу трафіку та регулярного аудиту вразливостей [3]. Подальші дослідження у цьому напрямі мають бути спрямовані на розробку інтелектуальних систем виявлення аномалій на основі штучного інтелекту, здатних запобігати деструктивним кібератакам у режимі реального часу.

Список використаних джерел

1. Кузнецов С. В., Бондаренко О. М. Кібербезпека критичної інфраструктури та автоматизованих систем управління : монографія. Київ : Техніка, 2024. 245 с.

2. Сдіховська О. Є., Бєлоусов В. С. Захист інформації в автоматизованих системах управління технологічними процесами. Системи управління, навігації та зв'язку. 2025. Вип. 2 (72). С. 112–118.

3. Guide to Operational Technology (OT) Security : NIST Special Publication 800-82 Rev. 3 / National Institute of Standards and Technology. 2023. 250 p.

4. Byres E., Lowe J. The Myths and Facts of Secure SCADA Networks. Proceedings of the 5th Annual IEEE Information Assurance Workshop. 2024. P. 38–45.

УДК 004.056

КІБЕРБЕЗПЕКА ТА ЦИФРОВА ГІГІЄНА

Максим Дякунчак

Миколаївський національний аграрний університет, м. Миколаїв, Україна

Науковий керівник: Л. О. Борян,
старший викладач Миколаївський національний аграрний університет

Цифрові технології стали невід’ємною частиною повсякденного життя людини. Інтернет використовується для навчання, спілкування, роботи, здійснення покупок, користування банківськими та державними сервісами. Водночас активне використання цифрових ресурсів супроводжується зростанням кількості кіберзагроз. Однією з найпоширеніших є фішинг - спосіб шахрайства, за якого зловмисники намагаються змусити користувача добровільно передати конфіденційну інформацію, зокрема паролі, коди підтвердження або банківські дані. Тому кібербезпека та цифрова гігієна мають бути важливою складовою поведінки кожного користувача.

Цифрова гігієна - це сукупність повсякденних правил і звичок, спрямованих на безпечне використання цифрових пристроїв, сервісів та інформації. Її основою є відповідальне ставлення до власних облікових записів і персональних даних. Насамперед користувачеві необхідно створювати складні та унікальні паролі для різних сервісів. Використання одного пароля на декількох сайтах збільшує ризик компрометації одразу кількох облікових записів. Для додаткового захисту доцільно використовувати багатофакторну автентифікацію, якщо вона доступна.

Важливою складовою цифрової гігієни є також своєчасне оновлення операційної системи, браузера та встановлених програм. Оновлення можуть містити виправлення вразливостей, які потенційно можуть бути використані зловмисниками. Не менш важливо встановлювати програми лише з надійних джерел, перевіряти дозволи, які надаються застосункам, та не відкривати підозрілі файли.

Особливу увагу слід приділяти протидії фішингу. Фішингові повідомлення можуть надходити електронною поштою, у соціальних мережах, месенджерах або у вигляді SMS. Зловмисники часто використовують повідомлення про нібито заблокований акаунт, проблеми з оплатою, необхідність підтвердити особу або отримати винагороду. Для підвищення довіри вони можуть копіювати логотипи, стиль оформлення та назви відомих компаній.

Перед переходом за посиланням потрібно перевірити адресу вебсайту та переконатися, що вона відповідає справжньому домену сервісу. Не слід вводити пароль, реквізити платіжної картки або