DOI: 10.58254/viti.7.2025.14.147

УДК 519.876.5:004.056:004.491.42

д-р техн. наук, професор Савченко В. А. ORCID: 0000-0002-3014-131X (ДУІКТ)
Хавер А. В. ORCID: 0009-0003-4731-914X (ДУІКТ)

МЕТОД РОЗРАХУНКУ КІБЕРСТІЙКОСТІ 2-1 РІВНІВ МОДЕЛІ PURDUE ПРОТИ СПЕЦІАЛІЗОВАНОГО ТЕХНОЛОГІЧНОГО ТРОЯНСЬКОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Забезпечення кіберстійкості об'єкта критичної інформаційної інфраструктури, зокрема його технологічної системи, є одним з основних завдань, яке стоїть перед керівництвом сучасних державних і приватних підприємств як в Україні, так і світі загалом.

Кібератаки на технологічні системи об'єктів критичної інфраструктури зазвичай здійснюються хакерськими групами (суб'єктами кіберзагрози), які спонсоруються зацікавленими державами. Метою такої кібератаки може бути як кібершпигунство, так і здійснення деструктивного кібервпливу на фізичні виробничі системи підприємства, що може загрожувати значними фінансовими збитками, зупинкою технологічного процесу й навіть техногенними катастрофами. Головним інструментом, із використанням якого суб'єктами кіберзагрози здійснюються такі кібератаки, є спеціалізоване технологічне троянське програмне забезпечення.

Інформаційні системи об'єкта критичної інфраструктури поділяються на комунікаційну та технологічну системи (які ще прийнято називати корпоративною та промисловою відповідно), кожна з яких є об'єктом критичної інформаційної інфраструктури. Найбільш небезпечною є кібератака на 2-1 рівні (згідно з моделлю Purdue) технологічної системи об'єкта критичної інфраструктури. Це зумовлено тим фактом, що на 2-1 рівнях моделі розгорнуті та функціонують найбільш важливі інформаційні підсистеми технологічної системи об'єкта критичної інфраструктури – Basic Process Control Systems і Safety Instrumented Systems. Кіберстійкість Safety Instrumented Systems є ключовим елементом кіберстійкості технологічної системи об'єкта критичної інфраструктури.

Ключові слова: *метод, кібербезпека об'єктів критичної інформаційної інфраструктури, кіберстійкість, спеціалізоване технологічне троянське програмне забезпечення, технологічна система, Basic Process Control Systems, Safety Instrumented Systems, Supervisory Control and Data Acquisition, рішення промислового кіберзахисту.*

V. Savchenko, A. Khaver. Method for calculating the cyber resilience of levels 2-1 of the Purdue model against specialized technological trojan software

Ensuring the cyber resilience of a critical information infrastructure facility, particularly its technological system, is among the primary the primary responsibilities of the management of modern public and private enterprises, both in Ukraine and globally.

Cyberattacks targeting the technological systems of critical infrastructure facilities are typically conducted by hacker groups (cyber threat actors) sponsored by state entities. The objectives of such cyberattacks may include both cyber espionage and destructive cyber impacts on an enterprise's physical production systems, potentially leading to substantial financial losses, disruption of technological process and even man-made disasters. The principal tool employed by cyber threat actors to execute such cyberattacks is specialized technological Trojan software.

The information system of a critical infrastructure facility are divided into communication and technological systems (also called corporate and industrial, respectively), each of which is an object of critical information infrastructure. The most dangerous is a cyberattack at level 2-1 (according to the Purdue model) of the technological system of a critical infrastructure facility. This is due to the fact that the most important information subsystems of the technological system of a critical infrastructure facility are deployed and operate at levels 2-1 of the model - Basic Process Control Systems and Safety Instrumented Systems. The cyber resilience of the Safety Instrumented Systems constitutes a critical component of the overall cyber resilience of the technological system of a critical infrastructure facility.

Keywords: *method, cybersecurity of critical information infrastructure facilities, cyber resilience, specialized technological Trojan software, technological system, Basic Process Control Systems, Safety Instrumented Systems, Supervisory Control and Data Acquisition, industrial cybersecurity solutions.*

Постановка завдання. В умовах, коли кіберстійкість об'єктів критичної інформаційної інфраструктури (далі – ОКІІ) є критично необхідною умовою переваги держави як протиборчої одиниці в кіберпросторі, важливим є забезпечення її високого рівня щодо технологічних систем об'єктів критичної інфраструктури держави та забезпечення

належного кіберзахисту проти деструктивного кібервпливу. Деструктивний кібервплив – це кібератака, метою якої є пошкодження або знищення даних, апаратної та/або програмної складової комунікаційної або технологічної системи (зазвичай об’єкта критичної інфраструктури), порушення її сталого функціонування та/або порушення функціонування елементів, що входять до її складу.

Аналізуючи найбільш резонансні та складні кібератаки на ОКІІ впродовж останнього десятиліття, які мали на меті деструктивний кібервплив, можна зробити висновок, що необхідною передумовою до їх успішного проведення було отримання доступу до керування критичними функціями Safety Instrumented Systems. Цей факт підтверджують численні звіти провідних дослідних компаній у галузі кібербезпеки щодо кібератаки “Blackenergy” (2015 р.), “Industroyer”/“Industroyer v2” (2016 р., 2024 р.), “Triton” (2017 р.) та ін. Заразом всі вони були здійснені з використанням спеціалізованого технологічного троянського програмного забезпечення (далі – СТТПЗ). Автором пропонується наступна дефініція терміну СТТПЗ – це вид кіберзброї, що маскується від засобів виявлення та/або імітує легітимне програмне забезпечення, має функції віддаленого управління та призначене для застосування в конкретній технологічній системі/конкретних типах технологічних систем (з урахуванням технологічних особливостей будови інформаційних систем) з метою здійснення кібершпигунства чи/та деструктивного кібервпливу.

Крім того, дотепер у науковому середовищі спостерігається помітний дефіцит досліджень та публікацій щодо підвищення кіберстійкості головних інформаційних підсистем технологічних систем, зокрема Basic Process Control System і Safety Instrumented Systems, та висвітлення ймовірних негативних наслідків впливу на технологічний процес від суб’єктів кіберзагрози на вищезазначені підсистеми.

За даними MITRE ATT&CK for Industrial Control Systems: Design and Philosophy, найчастіше ціллю хакерів у технологічній системі є наступні три основні інформаційні підсистеми рівня 3 і нижче моделі Purdue: Basic Process Control Systems (далі – BPCS), Safety Instrumented Systems (далі – SIS), Engineering and Maintenance Systems (далі – EMS). Модель Purdue (Purdue Enterprise Reference Architecture (“PERA”/”ISA-99”), далі – модель) – еталонна модель сегментації комунікаційної та технологічної систем.У контексті даної публікації здійснюється дослідження на 2-1 рівнях моделі Purdue (Control Systems Zone – Basic controls Zone).

Варто зауважити, що у разі, якщо кібератака здійснюється суб’єктом кіберзагрози з метою кібершпигунства, то найчастіше вона буде поширюватися на рівні моделі не нижче другого. Це обґрунтовано тим фактом, що саме другий рівень моделі є найнижчою ланкою технологічної мережі, на яку може поширитися кібератака з метою отримання технологічних даних, так як нижче дані щодо діяльності підсистем технологічної мережі не є структурованими, отже їх аналіз ускладнюється та не є виправданим. У свою ж чергу деструктивна кібератака з високою долею ймовірності може поширитися на перший рівень моделі (що залежить від кінцевої мети такого деструктивного кібервпливу).

Аналіз літератури. Аналіз останніх наукових досліджень і публікацій щодо кібербезпеки технологічних систем об’єктів критичної інфраструктури та їх складових, зокрема кібербезпеки Safety Instrumented Systems (далі – SIS), вказує на те, що за даним вектором активно проводять свої дослідження як українські, так й іноземні науковці.

Серед українських науковців (за результатами аналізу публікацій на платформах “Scopys” та “Web of Science”) питаннями кіберзахисту технологічних систем, у тому числі на 2-1 рівнях моделі, займаються [1–3] та інші. Спрямування досліджень зазначених авторів пов’язані з підвищенням кібербезпеки технологічних систем, в тому числі в окремих дослідженнях із використанням підходів машинного навчання.

Серед іноземних науковців питання кіберзахисту SIS на об’єктах критичної інфраструктури морських нафтових родовищ (в нафто-, газовидобувному секторі) підіймаються у дослідженнях [4]; із проблематикою ідентифікації кіберризиків для контрольно-вимірювальних систем та SIS пов’язані наукові дослідження [5]; дослідженнями рішень кібербезпеки для цифрових контрольно-вимірювальних приладів і систем керування на об’єктах ядерної енергетики займалися [6]. Серед вищеперерахованих досліджень не було запропоновано конкретного рішення для покращення такого показника кіберстійкості Safety Instrumented System, як стійкість перед СТТПЗ.

Мета та завдання дослідження. Розробка методу розрахунку кіберстійкості 2-1 рівнів моделі проти спеціального технологічного троянського програмного забезпечення.

Основними завданнями дослідження є:

– вибір взаємоархітектури між BPCS і SIS для оптимальної підтримки кібербезпеки технологічного процесу;

– проаналізувати тактики, які можуть бути використані суб’єктом кіберзагрози при експлуатації СТТПЗ для деструктивного кібервпливу на SIS;

– дослідити існуючі методи (підходи) до забезпечення кіберзахисту технологічних систем на основі обраних пропрієтарних програмних рішень промислового кіберзахисту (з використанням інформації з офіційної технічної документації виробника), визначити їх сильні/слабкі сторони та загальні підходи до їх функціонування;

– розрахувати кіберстійкість для 2-1 рівнів моделі.

Основна частина

1. Аналізуючи особливості кіберзахисту технологічної системи на 2-1 рівнях моделі (де розгорнуто основні інформаційні підсистеми BPCS і SIS) важливо розглянути її типову архітектуру та в подальшому, спираючись на неї, виділити окремі вектори кіберзагроз, характерні на цих ланках технологічної системи (рис. 1).

Другий рівень моделі зазвичай починається з фаєрволу (програмного/апаратного його рішення), що розділяє 3 і 2 рівень моделі між собою. Через фаєрвол здійснюється комунікація 2 рівня моделі з вищими рівнями моделі та, можливо, враховуючи конкретну реалізацію, із системами, які розгорнуті в сегменті комунікаційної мережі, наприклад, системою виконання виробництва (MES) і системами планування ресурсів підприємства (ERP) *(в подальшому дослідженні таку взаємодію будемо ідентифікувати як вектор загрози “згори”).*

Безпосередньо на 2-му рівні моделі розгорнуто верхні рівні управління ключовими інформаційними підсистемами технологічної системи (Industrial Control System, далі – ICS) – BPCS і SIS.

BPCS – це інформаційна підсистема ICS, яка функціонує на 2-1 рівнях моделі, має безпосередній вплив на 0 рівень моделі та призначена для здійснення моніторингу стану технологічного (виробничого) процесу та управління ним. SIS – це інформаційна підсистема ICS, яка функціонує на 2-1 рівнях моделі, має вплив на 0 рівень моделі та призначена для забезпечення безпеки експлуатації технологічного об’єкта, контролю аварійних процедур і, у разі виникнення аномалій, приведення технологічного процесу до безпечного стану. Міжнародним стандартом, що визначає вимоги кібербезпеки для систем BPCS і SIS, є IEC 62443.

На 2-му рівні моделі вищезазначені підсистеми можуть бути представлені такими програмно-апаратними засобами:

BPCS: сервер Supervisory Control and Data Acquisition (SCADA)/сервер Distributed Control System (DCS), Human-Machine Interface (HMI), інженерне робоче місце (робоче місце оператора/Engineering Workstation);

SIS: головний контроллер безпеки (Safety Controller), Human-Machine Interface (HMI), інженерне робоче місце (робоче місце оператора/SIS Engineering Workstation).

Враховуючи підходи до політики безпеки ОКІІ, на 2-му рівні моделі може бути реалізовано доступ до мережі Інтернет або він може бути заборонений. Зокрема, доступ до мережі Інтернет може бути здійснено для реалізації можливості віддаленого доступу для адміністратора SCADA/DCS (згідно з рекомендованими практиками в такому разі має бути застосовано багатофакторну автентифікацію).

Окрім того не виключається, що інформаційні підсистеми рівня 2 можуть отримати несанкціоноване з’єднання з мережею Інтернет через неналежне ставлення персоналу до інформаційної безпеки підприємства (*в подальшому дослідженні таку взаємодію будемо ідентифікувати як вектор загрози “з середини”)*. Крім того, при наявності Інтернет-з’єднання з робочою станцією, на якій є застаріле вразливе програмне забезпечення, суб’єкт кіберзагрози потенційно може отримати ще одну точку входу в технологічну систему. Разом з тим, все частіше зустрічаються випадки, коли користувачі інженерної станції через доступ до мережі Інтернет здійснюють доступ до вебсайту постачальника послуг, на якому суб’єкти кіберзагроз реалізують тип кібератаки “перехоплення ланцюжка поставок” через постачальників спеціалізованого програмного забезпечення (*в подальшому дослідженні таку взаємодію будемо ідентифікувати як вектор загрози “ззовні”).*

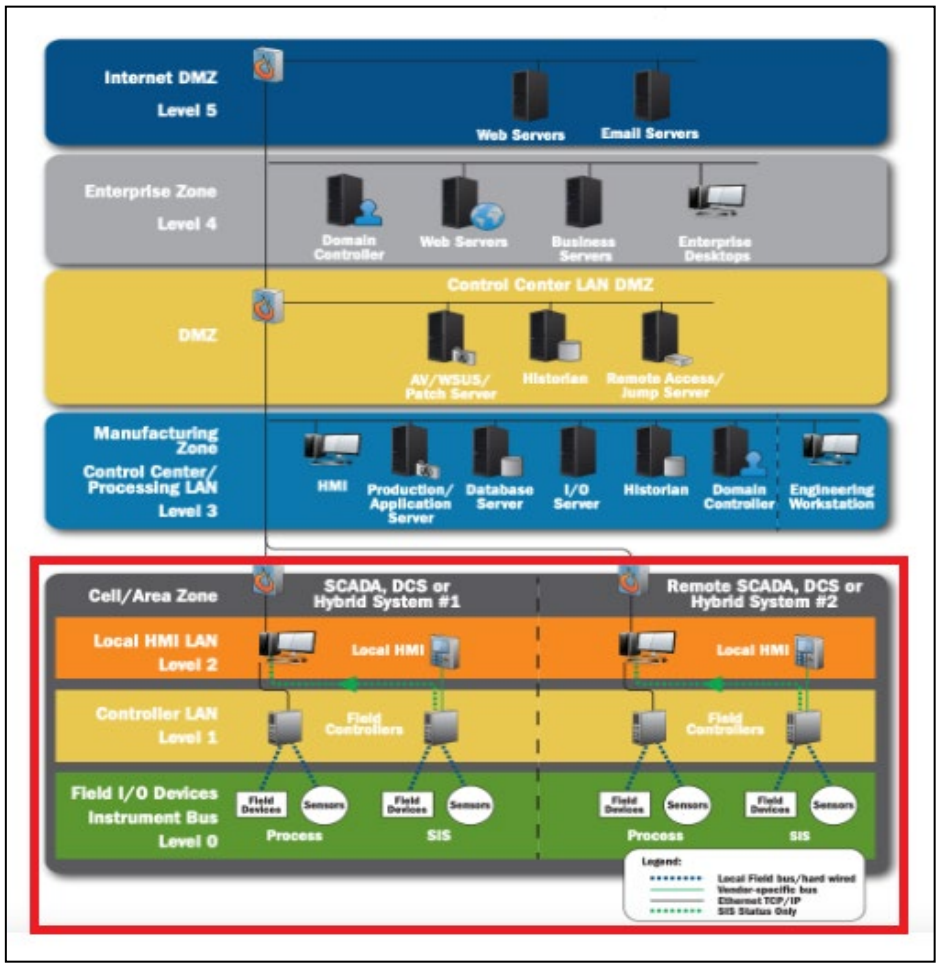

Рис. 1. Структурна схема реалізації моделі Purdue
(червоною рамкою виділено 2-0 рівні моделі Purdue, щодо яких проводиться подальше дослідження)

На 1-му рівні моделі підсистема BPCS представлена рядом контролерів (які мають зв'язок із сервером SCADA/DCS), до яких підключено сенсори, що знаходяться нижче за ієрархією на 0 рівні моделі. До цих же контролерів на другому рівні підключені і виконавчі механізми, які теж знаходяться на рівні 0. Такі підсистеми BPCS, як Support Skids та підсистема розподілу потужності (Power distribution), розгорнуті на 1-0 рівнях моделі.

SIS, зі свого боку, на 1 рівні моделі представлена головним контролером безпеки (Safety Controller), службовими контролерами безпеки, підсистемою розподілу потужності (окремо для роботи SIS, не є обов'язковою, але є рекомендованою), що живить контролери та сенсори, виконавчі механізми (які знаходяться на 0 рівні моделі) та підтримує роботу SIS у разі збоїв у централізованому енергопостачанні.

Згідно з вищерозглянутою архітектурою на рівні 1 моделі, початковою точкою входу в технологічну систему є контролер. Отримати доступ до нього суб'єкт кіберзагрози може у разі, якщо контролер має доступ до мережі Інтернет, або з середини технологічної мережі. З середини технологічної мережі отримати доступ до контролера можна фізично або завдяки використанню ряду технік бокового переміщення.

Не виключається також ризик доступу суб'єктом кіберзагрози з 0 рівня моделі до 2-1 рівнів моделі. Це, зокрема, можливо завдяки компрометації "розумних" сенсорів/виконавчих механізмів, фізичного доступу до фізичних інтерфейсів і бездротових мереж технологічної мережі, а також її пристроїв.

Між інформаційними підсистемами BPCS і SIS на 2-1 рівнях моделі присутній логічний та фізичний взаємозв'язок. Варіант такого зв'язку залежить від обраної архітектури реалізації і може бути виконаний в один із чотирьох способів. Від вибору правильної архітектури залежить рівень кіберстійкості SIS та відповідно вся безпека технологічного процесу, а також успішність ймовірної деструктивної кібератаки з використанням СТТПЗ.

Розглянемо типові можливі архітектури взаємодії BPCS і SIS, які можуть бути практично реалізовані на ОКІІ, та їх надійність з точки зору кібербезпеки.

Перший варіант реалізації архітектури між BPCS і SIS має назву "з повітряним зазором" (англ. "air gap"). Головною характеристикою такого підходу є те, що дві системи функціонують незалежно одна від одної, тобто є фізично й логічно ізольованими. Така архітектура взаємодії застосовується з метою мінімізації впливу кібератак, відмов, збоїв у BPCS на роботу системи безпеки (SIS). В такій реалізації підсистеми BPCS і SIS можуть обмінюватися лише даними про тривоги або сигналами про аварійну ситуацію.

Тобто, реалізація архітектури "з повітряним зазором" дозволяє ізолювати обидві системи одна від одної, проте для обміну критично важливими сигналами про аварійну ситуацію між ними зберігається одна спільна точка перетину (ймовірна точка входу суб'єкта кіберзагрози). Якщо ця точка перетину надійно захищена та враховано всі інші рекомендації до кібербезпеки SIS, така архітектура забезпечує найкращий рівень її кіберстійкості.

Другий варіант реалізації архітектури між BPCS і SIS має назву "інтерфейсний" (англ. "interface"). "Інтерфейсна" архітектура полягає у тому, що між BPCS і SIS використовуються спільні канали зв'язку та спільні протоколи (Modbus, Profibus, Ethernet/IP або HART), при цьому зберігається певний рівень ізоляції для критичних функцій SIS.

Отже, "інтерфейсна" архітектура забезпечує ізоляцію для критичних функцій, проте зберігає дві спільні точки перетину між BPCS і SIS (на рівні фізичного каналу та на рівні використання спільного протоколу), що забезпечує вплив на рівень кіберстійкості та дещо зменшує його порівняно з архітектурою "з повітряним зазором".

Третім підходом до архітектури між BPCS і SIS є "інтегрована" (англ. "integrated") реалізація. За такої архітектури BPCS і SIS є частинами єдиної системи та працюють у тісній взаємодії з використанням спільних фізичних каналів зв'язку, використовують спільні протоколи та дані для управління процесами. Не зважаючи на певні переваги така

архітектура збільшує кількість спільних точок перетину до трьох та не забезпечує достатнього рівня кіберстійкості SIS для ОКІІ.

Четвертим підходом щодо взаємодії між BPCS і SIS є “спільна” (англ. “common”) архітектура. Такий варіант реалізації побудований на використанні спільної платформи для роботи обох інформаційних підсистем. Це, в свою чергу, означає, що BPCS і SIS функціонують на спільних мережах, інтерфейсах, контролерах та, загалом, на спільному апаратному обладнанні. Проте між ними зберігається логічний розподіл функцій керування та безпеки за допомогою налаштованих конфігурацій і програмного забезпечення. Проте кількість спільних точок перетину в цій архітектурі є максимальною (з усіх вищеописаних підходів), що робить її найбільш вразливою до відмов і найменш кіберстійкою.

Варто зауважити, що міжнародні стандарти, такі як IEC 61511 і IEC 61508, не забороняють використання жодної з вищерозглянутих архітектур для BPCS і SIS, але залежно від кожної з реалізацій встановлюють жорсткі вимоги щодо забезпечення належного рівня розділення між цими системами. Проте при виборі архітектури реалізації варто враховувати всі вищезазначені потенційні ризики до збереження кіберстійкості SIS та перш за все враховувати категорію критичності об’єкта критичної інфраструктури, в технологічній системі якого її реалізовано.

Отже, розглянувши основне призначення, структуру, взаємоархітектуру та взаємодію BPCS і SIS можна зробити висновок, що у разі компрометації суб’єктом кіберзагрози елементів/складових BPCS (що у разі успішної деструктивної кібератаки може призвести лише до значних фінансових збитків і простою виробництва) єдиною перешкодою на шляху успішного здійснення масштабної деструктивної кібератаки є SIS (доступ до якої може завдати фізичного пошкодження механізмам та системам і навіть призвести до техногенних катастроф), яка контролює критичні параметри/функції безпеки технологічного процесу. Відтак доступ до SIS є основними пріоритетом суб’єкта кіберзагрози. Крім того, менш пріоритетним, але досить важливим на 2-1 рівнях моделі, є доступ до BPCS, підсистеми розподілу потужності та BPCS Support Skids, що може призвести до значних перебоїв у виробництві та збоїв в енергетичній мережі, хоча й менш серйозних, ніж втрата контролю над системами безпеки (SIS).

Для досягнення деструктивної кібератаки на технологічну мережу на 2-1 рівнях моделі суб’єкт кіберзагрози в якості інструменту кібератаки, майже напевно, буде використовувати СТТПЗ.

2. Розглянута будова 2-1 рівнів моделі описує важливість кіберстійкості підсистем BPCS та особливо SIS, а також окреслює потенційні точки входу суб’єкта кіберзагрози в технологічну систему, які дозволяють йому здійснити спробу деструктивної кібератаки з використанням СТТПЗ. Всі можливі техніки кібертатак, що стосуються ICS описані в методології для систем автоматизації та промислових процесів MITRE ATT&CK for ICS.

Серед усіх розглянутих в методології MITRE ATT&CK for ICS технік, рівнів 2-1 моделі стосуються наступні: T08800, T0830, T0878, T0802, T0895, T0803, T0804, T0805, T0806, T0892, T0807, T0885, T0884, T0879, T0809, T0893, T0813, T0814,T0868, T0816, T0871, T0820, T0890, T0866, T0823, T0874, T0877, T0872, T0826, T0880, T0829, T0835, T0831, T0832, T0849, T0838, T0836, T0839, T0801, T0834, T0840, T0842, T0861, T0845, T0886, T0846, T0888, T0847, T0848, T0851, T0852, T0853, T0881, T0856, T0869, T0862, T0894, T0857, T0863, T0859. Наведені техніки стосуються кібератак на апаратну, програмну та мережеву складові [9].

До найбільш небезпечних технік, що можуть призвести до деструкції/пошкодження компонентів SIS, можна віднести наступні: T0832, T0831, T0880, T0837, T0828, T0879.

Таким чином, потенційно суб’єкт кіберзагрози при виборі тактик і технік, за допомогою яких заплановано здійснення деструктивних кібердій щодо технологічної системи, має

значний арсенал, який дозволяє успішно реалізувати життєвий цикл СТТПЗ з 3 по 8.а етапи, що зображено на умовній схемі життєвого циклу СТТПЗ на рисунку 2 *(штрихпунктирною лінією на схемі рисунка 2 позначено не обов’язкові, проте можливі етапи життєвого циклу СТТПЗ)*.

3. Серед сучасних методів (підходів) до кіберзахисту технологічних систем у пропрієтарних рішеннях промислового кіберзахисту використовуються: сигнатурний аналіз, евристичний і поведінковий аналізи, а також їх комбінація/симбіоз з машинним навчанням, що дає змогу значно покращити захист від СТТПЗ та його виявлення в технологічній системі, починаючи з 3 по 5 етапи життєвого циклу (рис. 2).

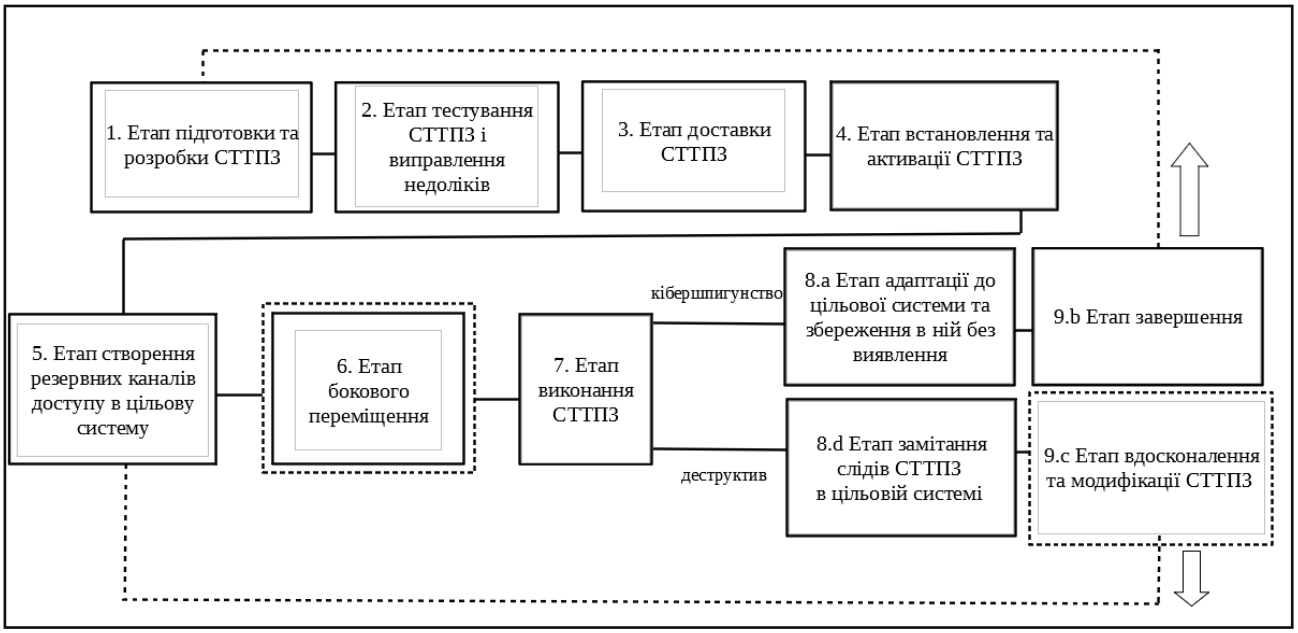

Рис. 2. Схема життєвого циклу СТТПЗ

Для аналізу можливості протидії СТТПЗ в технологічній системі розглянемо існуючі методи (підходи) на основі пропрієтарних рішень промислового кіберзахисту.

У процесі проведення подальшого дослідження було обрано рішення щодо кіберзахисту технологічних систем (в тому числі на 2-1 рівні моделі) Nozomi Networks Guardian (США) та Siemens SCADA and PLC Security (Німеччина). Ці продукти є найбільш популярними в своїй ніші та мають необхідні функціональні можливості, що відповідають завданню дослідження. Крім того, зазначені пропрієтарні рішення обрано з урахуванням їх реального використання на об’єктах критичної інфраструктури в різних географічних регіонах, що передбачає стратегічний підхід.

Nozomi Networks Guardian (далі – NNG). NGG призначене для моніторингу та управління компонентами (активним обладнанням) в технологічній системі.

Тип рішення NNG – NDR, безагентний підхід до збору даних із подальшою можливістю розгортання агентного компонента.

Розгортання NNG може бути здійснено на фізичному, віртуальному чи хмарному сервері. Після чого відповідний компонент NNG підключається до мережі та аналізує трафік, що передається між пристроями. Це дозволяє отримати детальну інформацію про активність і стан систем. З цією метою реалізується підключення до мережевого комутатора через порт віддзеркалення – Switched Port Analyzer (SPAN) або спеціальний пристрій TAP (Test Access Point). Інформацію з хостів (кінцевих пристроїв) NNG може отримувати завдяки режиму “Active Polling” (вимкнений за замовчуванням та потребує додаткової конфігурації), що

дозволяє збирати інформацію безпосередньо з пристроїв через SNMP, WMI, API, Syslog. А у разі, якщо необхідно ще більш детальне отримання інформації про кінцеві пристрої, передбачено додаткове встановлення агентної складової (наприклад, якщо потрібно зчитувати детальні журнали подій Windows-системи). Отже, архітектура рішення NGG передбачає значну гнучкість у питаннях рівня контролю як мережевого, так і хостового трафіку та подій.

На основі аналізу офіційної документації NNG можна зробити висновок, що рішення складається з таких 7 модулів та модуля, що є центральною системою управління: Nozomi Networks Guardian Sensor, Nozomi Networks Asset Intelligence, Nozomi Networks Threat Intelligence, Nozomi Networks Smart Polling, Nozomi Networks vGuardian, Remote Collectors, Guardian Air, Nozomi Networks Central Management Console. Варіант взаємодії елементів NGG по відношенню до моделі зображено на рисунку 3.

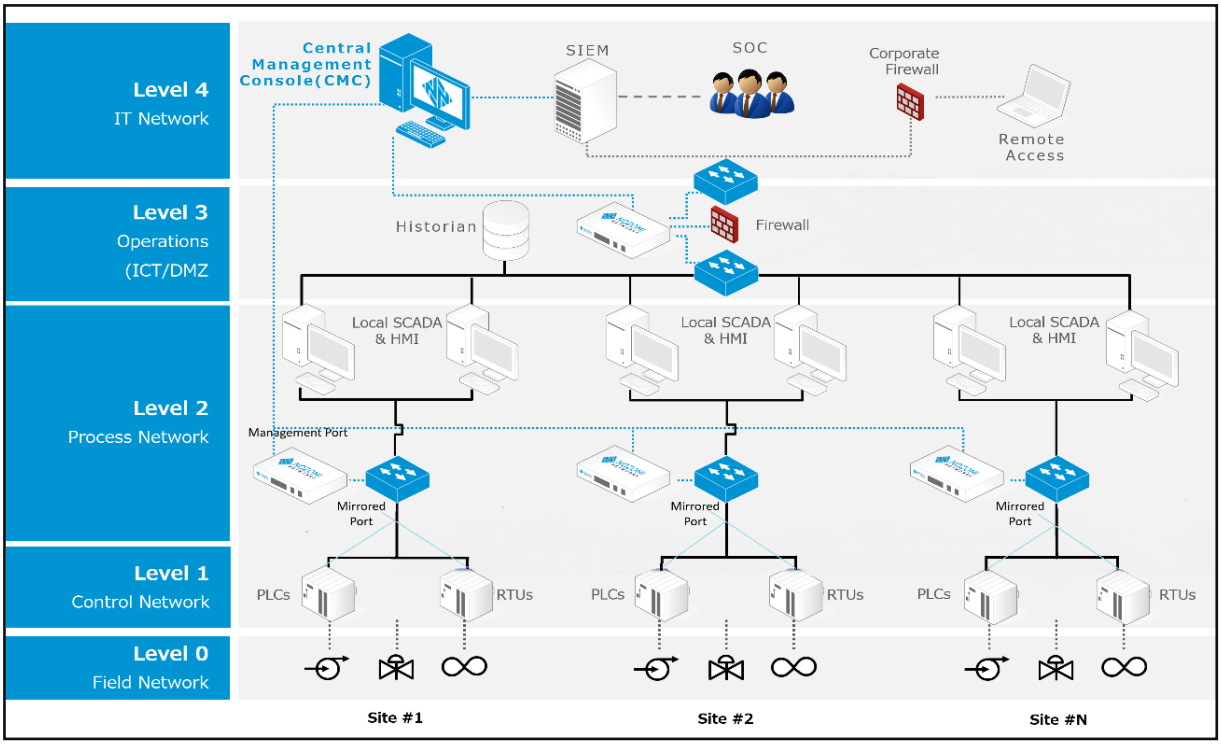

Рис. 3. Варіант взаємодії елементів NGG щодо моделі Purdue

Nozomi Networks Guardian Sensor як модуль відповідає за пасивний моніторинг трафіку через SPAN/TAP для виявлення аномалій, кібератак і вразливостей у технологічній мережі. Модуль автоматично виявляє та класифікує пристрої технологічної автоматизації нижчого рівня, аналізує поведінку пристроїв та створює базову модель нормальної роботи завдяки технології машинного навчання.

Nozomi Networks Asset Intelligence – автоматично виявляє та інвентаризує всі пристрої в мережі, збираючи детальну інформацію про їхні характеристики, конфігурацію, операційну систему, версію прошивки та можливі вразливості.

Nozomi Networks Threat Intelligence, як один із компонентів NGG, допомагає виявити нові типи атак або нестандартну поведінку на основі глобальних даних про загрози, використовуючи статистичні та алгоритмічні підходи.

Nozomi Networks Smart Polling – модуль призначений для опитування мережевих пристроїв і сенсорів для передачі цієї інформації до центральної системи управління, при цьому мінімізуючи навантаження на мережу та пристрої. Крім того, модуль використовує ML

для аналізу тенденцій та виявлення потенційних аномалій в поведінці пристроїв через SNMP, WMI або API.

Nozomi Networks vGuardian – модуль NGG, що призначений для роботи у віртуальному середовищі (наприклад, VMware ESXi, Microsoft Hyper-V) замість фізичного пристрою та розгортається у віртуальній інфраструктурі технологічної системи для моніторингу кібербезпеки технологічної мережі в частині кібербезпеки віртуальних робочих місць;

Remote Collectors – модуль, що відповідає за збір і консолідацію даних із віддалених сегментів мережі (на географічно розподілених локаціях) та передає ці дані до центральної системи управління (CMC).

Guardian Air – модуль NGG, який функціонує як автономний бездротовий сенсор безпеки, розроблений спеціально для технологічних середовищ, які активно використовують IoT. Цей сенсор безперервно моніторить бездротові технології в діапазоні від 800 МГц до 5895 МГц, включаючи Wi-Fi, Bluetooth, IEEE 802.15.4, LoRaWAN, Zwave, стільниковий зв’язок та дрони.

Nozomi Networks Central Management Console (далі – CMC) – є ключовим елементом NGG, його центральною системою управління, з якою взаємодіють усі модулі рішення, що забезпечує єдину, централізовану платформу для моніторингу, аналізу даних і реагування на загрози в технологічній системі [10].

Серед протоколів, які підтримує NNG, налічується близько шестисот варіантів.

Серед підходів до моніторингу мережевого сегмента NNG використовує такі технології як: Deep Packet Inspection (DPI), пасивне спостереження за трафіком (IDS), аналіз мережевих аномалій (Anomaly Detection), моніторинг зв’язків між пристроями (Network Mapping & Asset Discovery), контроль команд і дій у промислових протоколах (Protocol Whitelisting), машинне навчання.

Для моніторингу прикінцевого обладнання в NNG використовується: пасивне спостереження за мережевим трафіком від обладнання та побудова карти кінцевого обладнання, а також оцінка його вразливостей, поведінковий аналіз із застосуванням машинного навчання, аудит промислових протоколів.

Елементи машинного навчання присутні у таких модулях рішення NNG, як: Nozomi Networks Guardian Sensor, Nozomi Networks Asset Intelligence, Nozomi Networks Threat Intelligence. Це покращує характеристики виявлення аномалій і загроз, можливості для класифікації та інвентаризації пристроїв у технологічній мережі, можливості для виявлення досі невідомих загроз та мінімізує хибне спрацьовування (false positive).

Для роботи з віртуалізованою частиною інфраструктури технологічної системи в NGG передбачено використання віртуального образу рішення (наприклад, на віртуальних платформах VMware vSphere, Microsoft Hyper-V, Docker).

Крім того, NNG може інтегруватися з такими платформами та програмними рішеннями: SIEM (“Splunk”, “IBM Qradar”, “ArcSight”, “LogRhythm”), інструментами моніторингу (“Nagios”, “Zabbix”), системами управління подіями та інцидентами (“ServiceNow”, “BMC Remedy”), платформами для управління ризиками (“RSA Archer”, “MetricStream”), засобами виявлення та реагування на кінцевих пристроях (“CrowdStrike Falcon”, “Microsoft Defender for Endpoint”, “SentinelOne”, “Sophos Intercept X”, “Trend Micro Apex One”), платформами управління змінами та конфігураціями (“Ansible”, “SaltStack”), системами управління вразливостями (“Qualys”, “Tenable”, “Rapid7”), мережевими фаєрволами “Fortinet FortiGate”, платформою управління контейнерами “Docker”.

NNG підтримує алгоритми оновлення баз знань у технологічній мережі через центральну систему CMC або через базу вразливостей (наприклад, Національна база даних вразливостей). Причому оновлення через CMC може бути виконано одним із варіантів:

автоматично (як з виходом у мережу Інтернет, так і завдяки знімному носієві), вручну (завдяки вебінтерфейсу чи командному рядку).

NNG відповідає вимогам стандарту IEC 62443 [11].

Серед головних переваг рішення NNG (з точки зору забезпечення кіберстійкості на 2-1 рівнях моделі) – гнучкість у налаштуванні під конкретні потреби щодо моніторингу кібербезпеки, незначне навантаження на мережу та можливість додаткових поглиблених налаштувань моніторингу кінцевих точок у разі необхідності.

Окремої уваги при адмініструванні рішення NNG потребує контроль коректності конфігурацій (**Security Misconfiguration**), так як рішення має велику кількість взаємопов'язаних елементів архітектури. Така особливість може бути використана суб'єктом кіберзагрози у реалізації кібератаки **misconfiguration attack.**

Siemens SCADA and PLC Security (далі — SSPS). SSPS призначене для захисту технологічних систем від кіберзагроз, забезпечуючи безперебійність і безпечність технологічного процесу, акцентуючи свою увагу на кіберзахисті SCADA та PLC, відповідно на 2-1 рівні моделі. Варто зазначити, що перш за все рішення SSPS забезпечує максимальну свою ефективність в технологічній екосистемі "Siemens", завдяки максимальній взаємоінтеграції лінійки продуктів, що передбачає взаємну архітектуру. Проте рішення сумісне і з DCS, SCADA та PLC інших виробників. Крім того, рівень безпеки обладнання стороннього виробника буде залежати від закладених у нього виробником функцій безпеки та можливостей інтеграції з SSPS.

Основою підходу до забезпечення кібербезпеки у рішенні SSPS є класична стратегія "Defense in Depth", яка в технологічному сегменті передбачає комплексний підхід до питання забезпечення кібербезпеки на кожному фізичному/логічному контурі.

Тип рішення SSPS – комплексна система з інтеграцією функцій кіберзахисту в обладнання та програмне забезпечення систем керування.

SSPS складається з таких модулів: модуль безпеки PLC, модуль безпеки SCADA, інтегрований модуль кібербезпеки, модуль аудиту та моніторингу безпеки, модуль управління конфігураціями та оновленнями. Крім того, рішення має два ключових програмні інструменти, які є своєрідними централізованими компонентами "TIA Portal" та "WinCC".

Завдяки програмному компоненту "TIA Portal" інженери інтегрують в PLC модуль безпеки PLC та модуль управління конфігураціями.

"WinCC", в свою чергу, виконує функції SCADA-системи, забезпечуючи візуалізацію, моніторинг та аналіз даних, що надходять із різних модулів, таких як модуль безпеки SCADA, модуль аудиту та моніторингу безпеки. "WinCC" дозволяє операторам відстежувати стан технологічних процесів у режимі реального часу, реагувати на інциденти кібербезпеки та забезпечувати централізоване управління.

Обидва середовища взаємодіють із модулями SSPS через стандартизовані протоколи обміну даними (OPC UA, PROFINET, PROFIBUS та ін.), що дозволяє забезпечити комплексну безпеку, моніторинг та управління всією технологічною інфраструктурою [12].

Рішення SSPS дозволяє реалізувати єдину інтегровану екосистему, де "TIA Portal", "WinCC" та PLC працюють разом із вбудованими функціями кібербезпеки, що включають: сегментацію мережі та ізоляцію рівнів технологічної мережі; шифрування даних, що передаються між SCADA та PLC; контроль доступу та автентифікацію користувачів; захист від шкідливого програмного забезпечення; моніторинг загроз та інцидентів; захист від несанкціонованих змін у PLC та SCADA.

Модуль безпеки PLC працює на 1-му рівні моделі і призначений для: захисту логіки керування та коду PLC (запобігання несанкціонованому доступу до програмного коду контролера, використання технології Know-how Protection для шифрування програми, захист конфігурації контролера від несанкціонованої модифікації); контролю доступу (здійснюється

через багаторівневу систему аутентифікації, авторизації та управління правами користувачів); забезпечення функцій кібербезпеки PLC (програмно-апаратні фаєрволи вбудовані в PLC, шифрування даних та зв’язку), безпечного аварійного відключення (відповідно до вимог міжнародних стандартів ISO 13849-1, IEC 61508).

Модуль безпеки SCADA працює на 2-му рівні моделі, захищаючи взаємодію з вищим і нижчим рівнями та відповідає за: аутентифікацію та авторизацію (на основі використання надійних паролів, двофакторної автентифікації та інтеграції з корпоративними системами, наприклад, LDAP, Active Directory); моніторинг та виявлення загроз (моніторинг мережевих і системних подій на наявність аномалій та потенційних загроз із використанням інтеграції з рішеннями IDS/IPS, SIEM та ін.); шифрування та захист трафіку для безпеки взаємоз’єднань між сервером SCADA, HMI та PLC (на основі використання протоколів TLS, SSL, IPSec VPN), а також між SCADA-сервером і клієнтами (що особливо актуально у розподілених системах); моніторинг та аудит безпеки (логування подій, контроль змін конфігурацій, виявлення несанкціонованих підключень і підозрілих дій); інтеграцію з мережевими рішеннями безпеки (фаєрволами) для обмеження доступу в технологічну мережу.

Інтегрований модуль кібербезпеки у рішенні SSPS відіграє роль централізованої консолі управління. Даний модуль відповідає за: централізоване управління кібербезпекою (виступає централізованою консоллю для моніторингу та управління політиками безпеки для всієї технологічної екосистеми); кореляцію та аналіз даних (збирає інформацію з модулів безпеки PLC та SCADA, модуля аудиту та моніторингу безпеки, модуля управління конфігураціями та оновленням, а також із зовнішніх систем, таких як SIEM, IDS/IPS), що дозволяє оперативно виявляти аномалії та загрози (з використанням підходів машинного навчання); оперативне реагування на кіберінциденти (автоматизує процеси реагування на кіберзагрози, координує дії між різними модулями та допомагає ізолювати потенційні загрози, що здійснюється з використанням підходів машинного навчання); забезпечує інтеграцію й узгодженість політик кібербезпеки.

Модуль аудиту та моніторингу безпеки, зазвичай, розгортається на 2 рівні моделі та відповідає за систематичний збір, аналіз та зберігання інформації про події в системі. До основних функцій модуля належать: збір логів та подій (шляхом фіксування дій користувачів, змін у конфігурації, фіксуванні системних повідомлень та інших важливих подій з усіх компонентів системи); аналіз і кореляція даних (обробка зібраних даних для виявлення аномалій, підозрілих активностей або нетипової поведінки, що може свідчити про потенційні загрози, ймовірно, з цією метою у рішенні використовуються елементи машинного навчання); сповіщення та реагування (автоматичне генерування сповіщень і попереджень при виявленні підозрілої активності); аудит і забезпечення відповідності (проведення аудиту для перевірки на відповідність політикам кібербезпеки, ведення журналів подій).

Модуль управління конфігураціями та оновленнями у рішенні SSPS відповідає за систематичне керування та організацію контролю змін у програмному коді, зокрема: інтеграцію з іншими інформаційно-технологічними системами (забезпечує безпечний взаємообмін інформацією між різними системами); міграцію даних (забезпечує перенесення даних з існуючих систем, необхідних для впровадження та належної роботи системи SCADA та PLC); управління змінами та контроль версій (відслідковування змін у конфігураціях, зберігає початкову конфігурацію та веде історію змін); дозволяє автоматизувати процеси оновлення (централізоване управління оновленнями, в тому числі прошивками PLC).

Умовна схема взаємодії основних компонентів (модулів) рішення Siemens SCADA and PLC Securit зображена на рисунку 4.

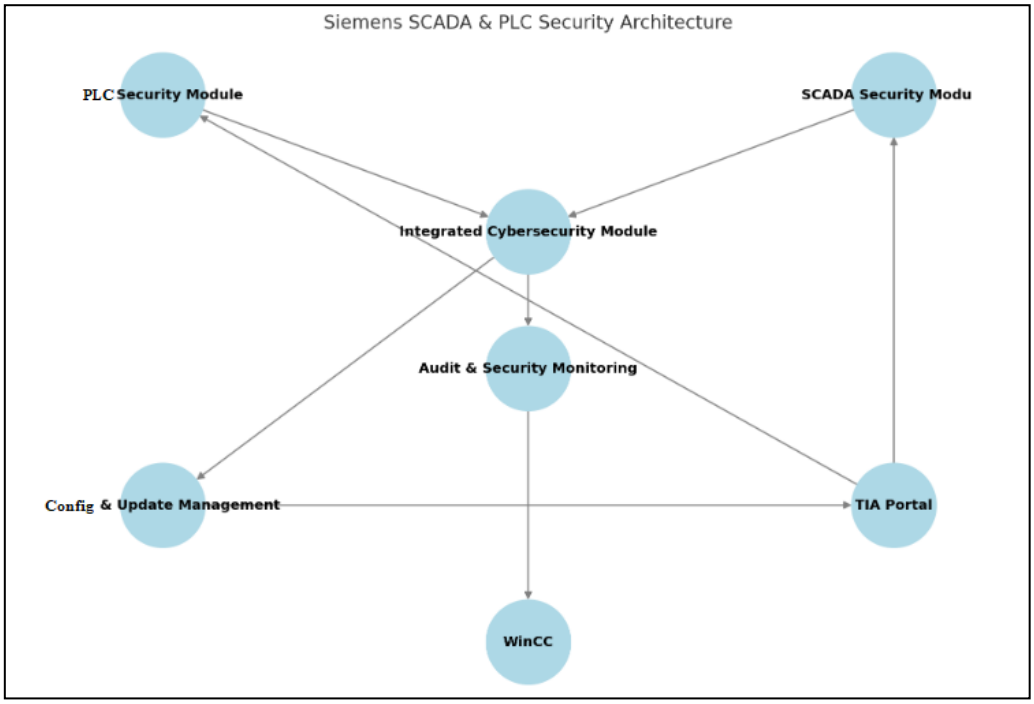

Рис. 4. Умовна схема взаємодії основних компонентів (модулів) рішення Siemens SCADA and PLC Security

Серед підходів до моніторингу мережевого сегмента SSPS використовує: інтеграцію з існуючими засобами кібербезпеки (фаєрволами, IDS/IPS, SIEM та іншими, що дозволяє SSPS ефективно інтегруватися в загальну архітектуру безпеки).

За моніторинг мережевого сегмента SSPS відповідає інтегрований модуль кібербезпеки. Він, зокрема, здійснює:

інтелектуальний моніторинг трафіку (включає DPI для виявлення аномалій на рівні промислових протоколів, сигнатурний аналіз, поведінковий аналіз, виявлення атак типу Man-in-the-Middle, а**втоматизоване реагування на загрози** через інтеграцію з SIEM та рішеннями для управління інцидентами (SOAR), що дозволяє блокувати підозрілу активність у реальному часі);

сегментацію мережі (завдяки використанню VLAN, DMZ, фаєрволів), моніторинг і контроль доступу (здійснюється інтегрованим модулем кібербезпеки та модулем аудиту й моніторингу безпеки);

швидку адаптацію до нових загроз через інтеграцію з програмами оновлення (через модуль управління конфігураціями та оновленнями) [13].

Серед підходів до моніторингу прикінцевого обладнання SSPS використовує: поведінковий аналіз; аудит і контроль доступу до пристроїв; моніторинг стану пристроїв та їх конфігурації; виявлення аномалій за допомогою машинного навчання; інвентаризацію та оцінку вразливостей; виявлення шкідливих програм; автоматизоване реагування та оркестрацію інцидентів (інтеграцію з SOAR для автоматизації процесів реагування на загрози, створення інцидентних маркерів і запуску сценаріїв ізоляції атак у реальному часі), централізоване логування, управління оновленнями, інтеграцію з рішеннями для управління кінцевими точками.

Серед модулів SSPS елементи машинного навчання містять такі: інтегрований модуль кібербезпеки (використовує машинне навчання для аналізу мережевого трафіку, виявлення аномалій і підозрілих патернів у промислових протоколах; допомагає адаптивно реагувати на нові загрози, знижуючи кількість хибного спрацьовування (false positive)); модуль аудиту та

моніторингу безпеки (використовує елементи машинного навчання для виявлення незвичної активності та кореляції подій безпеки; забезпечує аналіз журналів і змін у конфігураціях пристроїв для оперативного реагування на загрози).

Інтегрований модуль кібербезпеки SSPS може розгортатися у віртуалізованому середовищі, зокрема на платформі Microsoft Hyper-V, **VMware vSphere, Citrix Xen, KVM (Kernel-based Virtual Machine).**

Крім того, SSPS може інтегруватися з такими платформами: SIEM, інструментами моніторингу, SOAR, платформами для управління ризиками, засобами виявлення та реагування на кінцевих пристроях – Endpoint detection and response, платформами управління змінами та конфігураціями, системами управління вразливостями (офіційна документація не надає інформації щодо конкретних програмних рішень для інтеграції).

SSPS підтримує такі алгоритми оновлення баз знань у технологічній мережі: автоматичне оновлення через центральний сервер SSPS; оновлення через локальний репозиторій; через API та зовнішні джерела; оновлення в ручному режимі; контекстне (адаптивне) оновлення (відрізняється від традиційного автоматичного оновлення тим, що адаптується до локальних умов і може коригувати свою частоту та обсяг оновлень відповідно до змін у технологічній мережі).

Рішення SSPS відповідає вимогам стандарту IEC 62443.

Серед головних переваг рішення SSPS – надійність у моніторингу стану кібербезпеки на таких підсистемах, як BPCS і SIS, зокрема за критерієм швидкодії реакції. Крім того, однією з переваг є урівноважений розподіл навантаження між програмним і апаратним компонентами даного рішення промислового кіберзахисту, що дозволяє зберегти високий рівень ефективності і водночас не навантажувати мережу і кінцеве обладнання.

До недоліків SSPS можна віднести орієнтованість на технологічну та інформаційну інфраструктуру “Siemens”, отже моногенну інформаційну інфраструктуру.

Таким чином, кожне з розглянутих рішень промислового кіберзахисту (NNG, SSPS) може бути розгорнуто у технологічній системі (щонайменше за критерієм відповідності стандарту IEC 62443). Проте варто зауважити про доцільність вибору конкретного рішення зважаючи на факт закритості вихідного коду та потенційну можливість отримання доступу до критичної технологічної інформації з боку зацікавлених держав, що особливо актуально у світлі сучасної геополітичної нестабільності, в тому числі і для забезпечення кіберзахисту SIS (під час вибору програмних рішень для аналізу не було виявлено у відкритих джерелах окремого рішення кіберзахисту для SIS). Після аналізу архітектури та можливостей кожного з рішень можна сформулювати загальні підходи до їх функціонування:

архітектура системи: багатомодульна, з окремими модулями, що відповідають за кіберзахист прикінцевого обладнання, зокрема за захист пристроїв (PLC, HMI, сенсори, виконавчі механізми) через аналіз їхнього стану, конфігурації та інші) та мережі (забезпечують моніторинг мережевого трафіку, сегментацію мережі та взаємодію з іншими системами (наприклад, SIEM, IDS/IPS та інші). В модулях рішень присутня комбінація сигнатурного, евристичного та поведінкового аналізу. Концептуальний підхід до управління модулями передбачає наявність центральної консолі (доступ до функцій якої суб’єкта кіберзагрози потенційно є одним із найбільш небезпечних явищ для кіберстійкості технологічної системи 2-1 рівнів моделі, як для BPCS, так і для SIS);

елементи машинного навчання присутні в централізованих консолях та модулях, відповідальних за функції поведінкового аналізу та аналізу подій;

для функціонування модуля, який забезпечує моніторинг прикінцевого обладнання, використовуються: агентний підхід (забезпечує більш детальний моніторинг окремих пристроїв, що дозволяє глибокий аналіз та локальний контролю, проте може бути обмежений обчислювальними ресурсами пристроїв); безагентний підхід (є менш інвазивним,

дозволяючи отримувати інформацію через стандартні протоколи без необхідності встановлення додаткового програмного забезпечення на кожному пристрої, що особливо важливо для критичних компонентів SIS. Може здійснюватися, наприклад, через SNMP, WMI, API, Syslog).

Важливо зауважити, що при використанні типового підходу до управління модулями кіберзахисту в рішеннях промислового кіберзахисту, що передбачає наявність центральної консолі, здійснюється централізація управління. Такий підхід у єдиному для BPCS і SIS рішенні промислового кіберзахисту значно підвищує ризик несанкціонованого доступу суб'єкта кіберзагрози до компонентів SIS. З таких міркувань кібербезпеки на найбільш важливих ОКІІ доцільно децентралізувати управління системою промислового кіберзахисту і розгорнути в інфраструктурі SIS альтернативне рішення. Такий підхід підкріплено, зокрема, і рекомендаціями по розподілу або децентралізації архітектури "NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security" [14].

4. Враховуючи всі розглянуті особливості забезпечення кіберстійкості від СТТПЗ на 2-1 рівнях моделі (вектори можливих кібератак, взаємоархітектуру між BPCS і SIS, особливості функціонування промислових систем кіберзахисту), можна визначити загальну формулу кіберстійкості для 2-1 рівнів моделі.

Варто зауважити, що кіберстійкість 2-1 рівнів моделі у даному дослідженні як один з головних критеріїв пропонує враховувати сумарний показник кіберстійкості двох основних інформаційних підсистем, які функціонують на цих рівнях, відповідно BPCS і SIS. Крім того, в подальших розрахунках по замовчуванню буде вважатися, що архітектура самої SIS є максимально кіберстійкою.

Врахуємо, що загалом можливі три вектори здійснення кібератаки з використанням СТТПЗ на 2-1 рівні моделі (див. рис. 1):

"згори" – з рівнів комунікаційної системи, DMZ (рівень 3.5 моделі) та Manufacturing zone (рівень 3 моделі);

"ззовні" – через вихід у мережу Інтернет безпосередньо з 2-1 рівнів моделі або через атаку "перехоплення ланцюжка поставок" (коли СТТПЗ вже знаходиться на обладнанні чи програмному забезпеченні, яке встановлюється постачальником);

"з середини" – через інсайдера або некомпетентного оператора/інженера або іншого працівника (який може переносити СТТПЗ на власному пристрої чи накопичувачі, не знаючи цього).

Зазвичай, під час здійснення кібератаки з використанням СТТПЗ для підвищення ефективності заходів суб'єктом кіберзагрози активно буде відпрацьовуватися більш ніж один вектор.

Найменшу загрозу кіберстійкості технологічної системи на 2-1 рівнях моделі несе вектор "згори" (враховуючи кількість засобів захисту, які СТТПЗ необхідно подолати, щоб досягти рівня 2 моделі). Проте цей вектор здійснення кібератаки є найдоступнішим. Вирішити питання нейтралізації цього вектора кібератаки дозволяє використання діодів даних.

Середній рівень загрози кіберстійкості технологічної системи на 2-1 рівнях моделі несе вектор "ззовні", так як зазвичай, всі технічні системи захисту сконцентровані на протидії не типовому/шкідливому трафіку з мережі Інтернет. Проте згідно з останніми дослідженнями все частіше суб'єктами кіберзагрози використовується тактика "перехоплення ланцюжка поставок", яка дозволяє здійснити доступ до технологічної системи під прикриттям "довіреного джерела". Цю тактику можна охарактеризувати як загрозу високого рівня.

Крім того, загрозу високого рівня буде становити вектор "з середини", що насамперед пов'язано з отриманням фізичного доступу суб'єкта кіберзагрози або зацікавленої/некомпетентної особи до технологічної системи.

Запропонований метод розрахунку кіберстійкості 2-1 рівнів моделі проти СТТПЗ ґрунтується на науковому методі експертної оцінки.

Відповідно до робочого документа об'єкта критичної інфраструктури, який визначає модель кіберзагроз технологічній системі підприємства (наприклад, на основі методу Operationally Critical Threat Asset, and Vulnerability Evaluation – OCTAVE), здійснюється визначення критеріїв, які в подальшому будуть враховувати експерти при оцінці кіберстійкості 2-1 рівнів моделі.

Визначення вагового коефіцієнта кожного критерію здійснюється експертами на основі аналізу рівня важливості критерію для збереження кіберстійкості технологічної системи на 2-1 рівнях моделі.

Автор пропонує, що критерії та їх вагові коефіцієнти визначаються на підставі експертних висновків на основі методу Сааті за такою процедурою:

серед працівників, відповідальних за забезпечення кіберзахисту технологічної системи об'єкта критичної інфраструктури, відбираються найбільш кваліфіковані фахівці (експерти);

експертами здійснюється визначення критеріїв та їх вагових коефіцієнтів;

надані експертні оцінки узагальнюються з використанням статистичної медіани або медіани Кеммелі;

здійснюються відповідні розрахунки за запропонованою формулою.

Присвоємо кожній зі взаємоархітектур між BPCS і SIS (завдяки їхнім технічним характеристикам) сталий коефіцієнт кіберстійкості: "з повітряним зазором" – 4; "інтерфейсна" – 3; "інтегрована" – 2; "спільна" – 1.

Визначимо запропоновані автором критерії, які будемо враховувати при оцінці кіберстійкості 2-1 рівнів моделі:

1. Кіберстійкість рішення промислового кіберзахисту. Вважаємо за замовчуванням, що обране рішення є максимально ефективним від СТТПЗ. Його кіберстійкість буде оцінено як суму кіберстійкості кожного з його модулів. Оцінити кіберстійкість кожного з модулів пропрієтарного рішення досить важко (оскільки потрібно аналізувати архітектуру та навіть початковий код рішення, що зазвичай є закритими виробником), проте за необхідності можна здійснити умовну оцінку за відкритою інформацією, враховуючи, що оцінка кіберстійкості буде не точною, а скоріше орієнтовною/наближеною (ваговий коефіцієнт – 0,9).

2. Взаємоархітектура між BPCS і SIS (ваговий коефіцієнт – 0,8).

3. Коректність налаштувань усіх програмно-апаратних вузлів і систем кіберзахисту в рамках BPCS і SIS (ваговий коефіцієнт – 0,7).

4. Ефективність політики усунення вразливостей (ваговий коефіцієнт – 0,6).

5. Ефективність політики розмежування доступу (ваговий коефіцієнт – 0,5).

6. Фактор небезпеки перехоплення ланцюжка поставок (ваговий коефіцієнт – 0,4).

7. Фактор небезпеки зацікавленого у кібератаці користувача/інсайдера (ваговий коефіцієнт – 0,3).

Визначимо й опишемо загальну кіберстійкість для 2-1 рівнів моделі, враховуючи 2 можливі вектори здійснення кібератаки з використанням СТТПЗ ("ззовні", "з середини") та всі можливі варіанти взаємоархітектури між BPCS і SIS. Крім того, під час розрахунку важливо врахувати ваговий коефіцієнт кожного з елементів оцінки:

$$CR_{2\text{-}1} = w_1\left(\frac{Aarch}{4}\right) + w_2\left(\frac{1}{n}\sum_{i=1}^{n} xi\right) + w_3 N + w_4 U + w_5 D + w_6(1 - V_{ext}) + w_7(1 - Vi_{nt}),$$

де $CR_{2\text{-}1}$ – Cyber Resilience, показник кіберстійкості для 2-1 рівнів моделі. Чим вищий цей кінцевий показник, тим стійкіша система до зовнішніх та внутрішніх загроз;

$CR_{2\text{-}1}$ як унормована формула забезпечується відповідною вагою $(w_1 + w_2 + \ldots + w_7) \geqslant 1$, або $CR_{2\text{-}1} = 0{,}99$ для табличного значення;

$\sum w_i = 1$ (наприклад, 0,15 + 0,15 + 0,15 + 0,15 + 0,1 +0,15 + 0,15 = 1),

або $\sum w_i = 0{,}99$ для того, щоб $CR_{2\text{-}1} < 1$ і max 0,99 для табличного порівняння;

$\sum x_i \rightarrow (\frac{1}{n}\sum_{i=1}^{n} xi)$ – середнє значення кіберстійкості для різних модулів є нормованим, що дозволяє отримати об'єктивну оцінку для множинних факторів, що впливають на систему в межах [0,1];

w_n – вагові коефіцієнти, які визначають важливість кожного з факторів у розрахунку кіберстійкості. Вони використовуються для коригування впливу кожного параметра на загальну стійкість системи. Кожен ваговий коефіцієнт (w) задається експертно або на основі аналізу унікальності та важливості кожного фактора для цієї конкретної системи. Наприклад, для фактора, який має критичне значення, ваговий коефіцієнт може бути більшим (для обчислення рекомендується використовувати діапазон в межах від 0,1 до 1 ($w_i \in [0{,}1–1.0]$). Визначити вагу коефіцієнта можна за допомогою: експертної оцінки, емпірично (наприклад, через метод аналізу ієрархій або Analytic Hierarchy Process);

A_{arch} – визначає реалізовану взаємоархітектуру між BPCS і SIS. Так як тип взаємоархітектури впливає на стійкість до кібератак, а ізольовані архітектури можуть бути більш стійкими до них, визначено наступні сталі коефіцієнти: "з повітряним зазором" = 4; "інтерфейсна" = 3; "інтегрована" = 2; "спільна" = 1.

x_i – кількість модулів пропрієтарного рішення промислового кіберзахисту. Для кожного модуля надається певне значення (для обчислення рекомендується використовувати діапазон в межах від 0,1 до 1 ($x_i \in [0{,}1–1{,}0]$), яке оцінює кіберстійкість цього модуля. Загальна кіберстійкість рішення промислового кіберзахисту обчислюється як сума цих значень;

N – визначає рівень коректності налаштувань всіх програмно-апаратних елементів, що використовуються для кіберзахисту на 2-1 рівнях моделі. Значення N обчислюється за допомогою експертного методу чи аудиту налаштувань. Значення N може знаходитися в межах від 0,1 до 1,0 ($N \in [0{,}1–1{,}0]$);

U – визначає ефективність/коректність політики усунення вразливостей в ПЗ на 2-1 рівнях моделі. Значення U може знаходитися в межах від 0,1 до 1,0 ($U \in [0{,}1–1{,}0]$);

D – визначає ефективність/коректність політики контролю доступу та авторизації в системі. Враховує використання мультифакторної автентифікації, рольового контролю доступу (RBAC), обмеження прав доступу. Значення D може знаходитися в межах від 0,1 до 1,0 ($D \in [0{,}1–1{,}0]$);

Z – показник рівня внутрішньої стійкості або адаптивності. Значення Z може знаходитися в межах від 0,1 до 1,0 ($U \in [0{,}1–1{,}0]$);

V_{ext} – визначає оцінку ризику від кібератак на 2-1 рівень моделі "ззовні" (наприклад, кібератаки через мережу Інтернет та з використанням атаки через ланцюг постачання (supply chain attack). Значення V_{ext} може знаходитися в межах від 0,1 до 1,0 ($V_{ext} \in [0{,}1–1{,}0]$);

V_{int} – визначає оцінку ризику від кібератак на 2-1 рівень моделі "з середини" (наприклад, кібератаки, які потенційно можуть бути здійснені інсайдером або ненавмисно некомпетентним співробітником). Значення V_{int} може знаходитися в межах від 0,1 до 1,0 ($V_{int} \in [0{,}1–1{,}0]$).

Кінцевий результат обчислень запропоновано порівняти з наступною умовною шкалою (таблиця 1). Отже, формула $CR_{2\text{-}1}$ дозволяє гнучко адаптуватись до різних систем, одночасно враховуючи технічні та організаційні аспекти кіберзахисту. Для полегшення порівняння між системами або варіантами архітектури використовуємо універсальну шкалу оцінювання в діапазоні [0,1]. Врахування кількості модулів та їхньої кіберстійкості ($\sum x_i$ / n) забезпечує масштабованість формули, яка залишається коректною незалежно від кількості модулів у системі. Формула враховує два вектори атаки (зовнішній і внутрішній), що дозволяє комплексно оцінювати ризики.

Таблиця 1

Умовна шкала оцінювання показника кіберстійкості 2-1 рівнів моделі Purdue

№ з/п	Значення $CR_{2\text{-}1}$	Інтерпретація	Коментар
1	0–0,20	низька кіберстійкість	критичний стан кіберстійкості, відсутність достатнього контролю кібербезпеки, слабка взаємоархітектура, неефективні політики
2	0,21–0,40	середня	окремі елементи захисту працюють ефективно, але високі ризики кіберстійкості
3	0,41–0,60	задовільна (прийнятна)	задовільний рівень, потрібні вдосконалення
4	0,61–0,80	висока	достатній рівень кіберзахисту
5	0,81–0,99	дуже висока	реалізовано повний спектр засобів кіберзахисту

Висновки. Отже, запропонований метод оцінки кіберстійкості 2-1 рівнів моделі, побудований на зваженому аналізі ключових технічних і організаційних факторів, є практичним, адаптивним і орієнтованим на реальні кіберзагрози. Його можна застосовувати як інструмент внутрішнього аудиту, порівняльної оцінки або як підґрунтя для покращення кіберзахисту в технологічній системі ОКІІ.

З огляду на проведений аналіз та враховуючи проміжні **висновки** дослідження, можна підсумувати, що:

найбільшою кіберзагрозою для технологічної системи ОКІ є ураження суб'єктом кіберзагрози SIS (що, зазвичай, здійснюється з використанням СТТПЗ);

оцінка кіберстійкості 2-1 рівнів моделі потребує регулярного перегляду з урахуванням всіх актуальних кіберзагроз (відслідковування тенденцій до застосування нових тактик та технік хакерськими групами з метою здійснення кібершпигунства та деструктивного кібервпливу на ОКІ з метою здійснення превентивних заходів);

поряд із такими традиційними елементами кіберзахисту 2-1 рівнів моделі, як коректність здійснення налаштувань, політика усунення вразливостей та розмежування доступу, одними з найвагоміших чинників кіберстійкості є коректна реалізація взаємоархітектури між BPCS і SIS, а також вибір оптимального (за низкою індивідуальних критеріїв реалізації роботи технологічної системи, наприклад: час реакції/час затримки; збереження балансу між навантаженістю мережі і кінцевого обладнання; достатній рівень гнучкості налаштувань; ефективність захисту від СТТПЗ; можливості розгортання у гетерогенному середовищі; можливості роботи з віртуалізованими середовищами та ін.) рішення промислового кіберзахисту, яке здатне ефективно та своєчасно виявляти кіберзагрози, зокрема СТТПЗ у технологічному середовищі 2-1 рівнів моделі з використанням сучасних підходів (сигнатурний, евристичний та поведінковий аналізи в комбінації/симбіозі з машинним навчанням);

на ОКІ високого рівня критичності при можливості необхідно здійснити децентралізацію рішення промислового кіберзахисту між інформаційними екосистемами BPCS і SIS. Це передбачає розгортання альтернативного (як варіант ізольованого) рішення для SIS.

У випадку коли розгортання альтернативного рішення в SIS обмежується рядом причин (технічного, фінансового характеру та інші), доцільно розглянути варіант реалізації додаткового рівня кіберзахисту (наприклад, із використанням відкритих рішень інтелектуального аналізу даних і машинного навчання).

Майбутні шляхи досліджень. Подальші дослідження автор зосереджує на підвищенні рівня кіберстійкості SIS за допомогою розгортання рішення інтелектуального аналізу даних

і машинного навчання “WEKA” з використанням інструментів поведінкової аналітики та моделі Long Short-Term Memory (LSTM),

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Borychenko Olena, Cherniavskyi Anatolii, Muliarevych Oleksandr, Shelekh Yurii, Sabat Myroslav. Cybersecurity in the energy industry of Ukraine: protection measures and challenges in the context of energy security // Journal of Management & Technology. № 24 (4). P. 67–90.

2. Mnushka O., Savchenko V. Security Model of IOT-based Systems // Conference: 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), February 2020.

3. Kondratenko Yuriy, Atamanyuk Igor, Sidenko Ievgen, Kondratenko Galyna. Machine Learning Techniques for Increasing Efficiency of the Robot’s Sensor and Control Information Processing // MDPI sensors. January 2022.

4. Pengyu Zhu, Jayantha P. Liyanage. Cybersecurity of Safety Instrumented Systems in the Context of Digitalization: Some Issues and Challenges within Oil and Gas Production Assets // The 30th European Safety and Reliability Conference, 1-5 November 2020.

5. Iaiani Matteo, Cozzani Valerio. Identification of cyber-risks for the control and safety instrumented systems: a synergic framework for the process industry // Process Safety and Environmental Protection 172. February 2023.

6. Fan Zhang, J. Wesley Hines, Jamie B. Coble. A Robust Cybersecurity Solution Platform Architecture for Digital Instrumentation and Control Systems in Nuclear Power Facilities // Nuclear technology. October 2019. № 206 (1).

7. Лагун Ілона, Яцук Юрій. Супервізорні системи керування та збору даних: навч. посіб. Львів, 2025. 222 с.

8. Ackerman Pascal. Industrial Cybersecurity Second Edition. 2021. 800 p.

9. MITRE ATT&CK Tactics. URL: https://attack.mitre.org/tactics/ics.

10. Documentation Nozomi Networks Guardian. URL: technicaldocs.nozominetworks.com.

11. Nozomi Networks Guardian User Guide. URL: https://technicaldocs.nozominetworks.com/out/pdf-output/Guardian-User%20Guide.pdf.

12. Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices. URL: https://manuals.plus/m/eb19631ac50ad569431320d677d4783fa7ba4913e39b74170099b90ff17647c2.

13. WinCC OA Documentation. URL: https://www.winccoa.com/documentation/WinCCOA/latest/en_US/videos/security/security_basics_guideline.htm.

14. NIST. *Guide to Operational Technology (OT) Security (SP 800-82 Rev. 3).* URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pd.