КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.798
УДК 681.3.06:004.056:004.421.2

Пановик Уляна Петрівна
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних технологій
у видавничо-поліграфічних процесах
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID: 0000-0002-9663-4328
uliana.p.panovyk@lpnu.ua

ЗАХИСТ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ НА ОСНОВІ КОНЦЕПТУАЛЬНОЇ МОДЕЛІ З ФОРМАЛІЗОВАНОЮ ОЦІНКОЮ ЕФЕКТИВНОСТІ

Анотація. В умовах зростання кіберзагроз та впровадження цифрових технологій в управління виробничими процесами автоматизовані системи дедалі частіше стають об'єктами атак, що ставить питання забезпечення інформаційної безпеки на критичних рівнях. Особливо актуально це для середовищ SCADA, IIoT і MES, де використання окремих рішень без цілісної захисної архітектури призводить до появи вразливих зон і зниження ефективності реагування на інциденти. У статті представлено концептуальну модель захисту інформації, яка інтегрує контроль доступу, виявлення аномалій та шифрування критичних повідомлень, а також передбачає формалізовану оцінку ефективності на основі кількісних метрик. Методична основа дослідження охоплює структурне моделювання загроз, алгоритмічне проєктування захисних механізмів, реалізацію функціональних модулів у середовищі Python та моделювання поведінкових сценаріїв за допомогою згенерованих логів подій. Для оцінювання ефективності захисної моделі використовувалися показники коефіцієнта ризику, частки виявлених атак, ентропії доступу та середнього часу реагування. Алгоритми функціонують у режимі реального часу, реагуючи на події відповідно до заданої логіки: система блокує або обмежує підозрілі дії, активує шифрування критичних повідомлень і фіксує всі інциденти в журналі подій. Проведене моделювання підтвердило результативність запропонованої моделі: коефіцієнт ризику зменшився більш ніж удвічі, точність виявлення атак досягла 95–98%, а ентропія розподілу доступу зросла, що свідчить про більш рівномірне та безпечне управління правами. Запропонована модель формує багаторівневу архітектуру захисту, яку можна впровадити як у традиційних SCADA- і MES-системах, так і в інфраструктурах IIoT. Завдяки гнучкій структурі, відкритості реалізації та здатності до адаптації модель може бути масштабована під конкретні потреби підприємства й застосована в умовах обмежених ресурсів або у великих виробничих системах. Отримані результати демонструють практичну придатність моделі для забезпечення надійного захисту даних в умовах сучасного кіберсередовища.

Ключові слова: автоматизовані системи; інформаційна безпека; SCADA; IIoT; контроль доступу; виявлення аномалій; шифрування; концептуальна модель; ефективність захисту.

ВСТУП

У сучасних умовах цифрової трансформації виробництва автоматизовані системи (АС) стали фундаментальним елементом управління технологічними процесами. Вони охоплюють широкий спектр інструментів — від SCADA-рішень і систем MES до розподілених архітектур на базі IoT і IIoT. Завдяки тісній взаємодії апаратних компонентів, програмного забезпечення та мережевої інфраструктури такі системи значно підвищують ефективність і точність виробничих операцій. Проте водночас

зростає і кількість потенційних кіберзагроз, які можуть призвести до збоїв, втрати даних або несанкціонованого втручання в критичні функції. З огляду на це виникає об'єктивна потреба в побудові інтегрованих моделей захисту інформації, які забезпечували б стійкість, адаптивність і формалізовану оцінку ефективності захисних заходів у таких середовищах. Ці виклики формують необхідність глибшого аналізу наявних підходів і постановки завдання розроб універсальної моделі захисту автоматизованих систем.

Постановка проблеми. Автоматизовані системи управління (АСУ), що використовуються в промисловості, енергетиці, транспорті та інших критичних галузях, дедалі частіше стають об'єктами цілеспрямованих кіберзагроз. Розвиток індустрії 4.0 та інтенсивне впровадження технологій Інтернету речей (IoT), зокрема, в середовищах SCADA, MES і IIoT, супроводжується ускладненням інфраструктури, що, своєю чергою, створює нові вектори атак. Зловмисники отримують можливість здійснювати несанкціоновані підключення до контролерів, модифікувати логіку роботи виконавчих пристроїв, перехоплювати дані через незахищені канали або впливати на роботу програмного забезпечення шляхом ін'єкцій і шкідливого коду. Такі порушення можуть мати не лише економічні, а й технологічні або навіть катастрофічні наслідки.

Попри наявність великої кількості рішень у сфері інформаційної безпеки, більшість із них залишаються вузькоспеціалізованими. Часто застосовуються окремі механізми безпеки, наприклад, базова автентифікація, ізольоване шифрування даних або виявлення аномалій. Проте такі підходи зазвичай не передбачають їхньої взаємодії в межах єдиної захисної архітектури. Це призводить до утворення незахищених сегментів, зокрема, на рівнях передачі даних між сенсорами, PLC-контролерами та SCADA-компонентами. Додатково ускладнює ситуацію відсутність чітких критеріїв оцінки ефективності впроваджених заходів. Більшість рішень аналізуються лише якісно або на рівні функціонального тестування без застосування кількісних метрик ризику, швидкості реагування, рівня виявлення атак чи ентропії доступу.

У динамічно змінному середовищі, де з'являються нові пристрої, канали зв'язку і протоколи, необхідна концептуально нова модель безпеки. Вона має поєднувати декілька ключових функцій: контроль доступу на основі політик, аналітичне виявлення відхилень у поведінці компонентів та шифрування критичних повідомлень, а також містити формалізовану систему метрик, що дає можливість оцінювати ефективність роботи кожного блоку. Таким чином, постає потреба у створенні адаптивної, модульної, масштабованої та вимірюваної архітектури захисту, здатної інтегруватися в різні типи АС — від компактних IoT-рішень до повномасштабних SCADA-комплексів.

Аналіз останніх досліджень і публікацій. Проблематика кіберзахисту автоматизованих систем знаходить відображення в численних наукових публікаціях, що охоплюють як питання виявлення аномалій, так і захисту промислових мереж і протоколів. Зокрема, у [6], [7], [14] акцентовано на побудові моделей виявлення загроз у SCADA-середовищах. У [6] представлено підхід на основі моделювання переходів станів, тоді як у [14] реалізовано алгоритм машинного навчання для аналізу трафіку з використанням протоколу Modbus. Дослідження [7] демонструє ефективність таймінгового аналізу для виявлення аномальної поведінки в мережі SCADA. Попри глибину досліджень, зазначені праці не охоплюють повноцінні механізми контролю доступу або реагування на події в реальному часі.

У контексті захисту промислового Інтернету речей (IIoT) варто виокремити роботи [4], [5], [8]. У [4] описано тестове середовище для перевірки ефективності методів кіберзахисту в IIoT, з урахуванням симуляції атак. У [5] проведено огляд розумних IoT-систем, де розглядаються питання безпеки, конфіденційності та застосування

інтелектуальних технологій. Дослідження [8] зосереджується на шифруванні зображень в IIoT за допомогою клітинних автоматів, демонструючи нестандартні підходи до захисту мультимедійного трафіку. Щодо гібридних підходів до захисту промислових систем, у публікації [15] представлено комбінацію блокчейн-технологій та глибокого навчання для створення IDS у SDN-архітектурі. Автори [11] у своєму дослідженні пропонують концепцію Defence-in-Depth у IIoT для досягнення наскрізного захисту в Industry 4.0. Робота [13] розглядає виявлення атак на SCADA в умовах великих даних, що особливо актуально для розподілених систем.

Питання захисту інформації в MES-середовищах розглядаються у [2], [9], [10]. У [2] описано механізми безпеки телекомунікаційних мереж, які можуть застосовуватись і до MES-рішень. Матеріали [9], [10] зосереджуються на прикладних аспектах безпеки управлінських систем, підкреслюючи необхідність інтеграції з SCADA-компонентами та забезпечення цілісного контролю. Окремо варто згадати [3], де досліджено підходи до безпеки мереж IoT із використанням блокчейн, а також [12], [16], [17], які розкривають аспекти моделювання вразливостей, побудови онтологій загроз та застосування EDR-систем для захисту критичних сегментів АС.

Загалом, проаналізовані джерела демонструють широку варіативність технік захисту, але при цьому мають спільний недолік — фрагментарність реалізації. Більшість досліджень охоплюють лише один або два аспекти інформаційної безпеки: автентифікацію [3], шифрування [8], виявлення аномалій [6], [14] або аналіз протоколів [7], [12], не формуючи єдиної концептуальної архітектури. Крім того, у більшості випадків відсутня формалізована оцінка ефективності впроваджених рішень – метрики ризику, ентропії доступу, швидкості реагування або частоти виявлення атак не подаються або мають якісний характер.

Отже, виокремлюється загальна науково-практична проблема — потреба в інтегрованій моделі, яка не лише об’єднує ключові захисні механізми, а й містить формалізовані критерії оцінювання їхньої ефективності для застосування в SCADA, IIoT та MES-середовищах.

Мета статті. Метою статті є розроблення концептуальної моделі захисту інформації для автоматизованих систем, що поєднує ключові захисні функції – контроль доступу, виявлення аномалій та шифрування повідомлень, у єдину архітектуру з алгоритмічною логікою, а також впровадження формалізованих метрик (ризик, ентропія, час реакції) для кількісного оцінювання ефективності цієї моделі.

МЕТОДИКА ДОСЛІДЖЕННЯ

На початковому етапі дослідження було сформовано типову архітектуру автоматизованої системи, що відображає її ключові структурні елементи: сенсори збору даних, програмовані логічні контролери (PLC), мережеву інфраструктуру (Ethernet/Modbus/TCP), SCADA/HMI-рівень, а також зовнішні канали передачі даних (включно з хмарними інтерфейсами та мобільним доступом). Модель будується із застосуванням принципу зонування за рівнем критичності і вразливості. У результаті побудови моделі створено архітектурну схему загрозоорієнтованої АС (рис. 1).

На основі побудованої загрозоорієнтованої моделі автоматизованої системи було здійснено формалізацію основних типів загроз, які найчастіше трапляються в контексті SCADA, IIoT та MES. Для кожного типу загроз визначено джерело, механізм дії, ймовірність реалізації, а також відповідні засоби протидії, що можуть бути реалізовані

на програмному або апаратному рівні. Такий підхід дає змогу здійснити структурований аналіз ризиків та пов'язати їх із конкретними точками впливу в архітектурі системи. У табл. 1 наведено типові загрози, характерні для кожного функціонального рівня, та засоби їхньої нейтралізації.

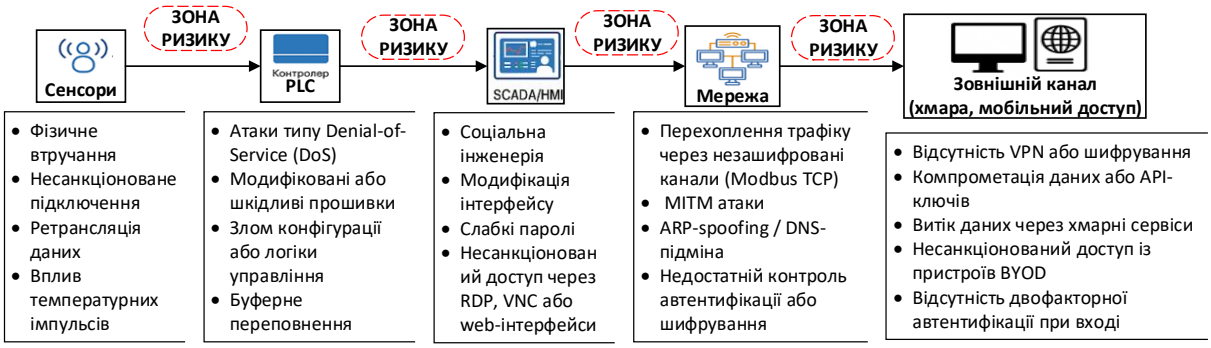

Рис. 1. Загрозоорієнтована архітектура автоматизованої системи

Таблиця 1

Формалізована відповідність типових загроз і засобів захисту

Рівень системи	Тип загрози	Приклад атаки	Основний механізм захисту
Сенсори	Підміна або блокування сигналу	Підключення фальшивого датчика	Фізичний контроль, MAC-фільтрація, списки дозволених пристроїв
Контролери (PLC)	Зміна логіки, DoS	Завантаження шкідливої прошивки	Аутентифікація, контроль доступу
Мережа передачі даних	Перехоплення, атака «людина посередині»	Sniffing, Packet injection	Шифрування, VPN, TLS/DTLS
SCADA/HMI	Зовнішній вплив, Social Engineering	Модифікація інтерфейсу	Двофакторна автентифікація, логування
Зовнішній канал	Несанкціонований доступ	Витік даних через API	Доступ на основі токенів, зворотний проксі (Reverse Proxy)

Кожен із описаних механізмів захисту може бути реалізований як окремо, так і в комбінації з іншими для досягнення ефекту Defense-in-Depth (багаторівневого захисту). Наприклад, одночасне використання TLS-тунелювання для мережевого трафіку та механізмів виявлення аномалій для контролю поведінки пристроїв дозволяє значно знизити ймовірність успішної атаки.

Розроблена концептуальна модель захисту інформації в автоматизованих системах передбачає поетапну реалізацію трьох ключових механізмів безпеки: *контролю доступу, виявлення аномальної активності* та *забезпечення конфіденційності даних через шифрування*. Кожен із цих механізмів реалізується як окремий логічно ізольований модуль, який отримує вхідні події із вразливих точок архітектури системи, обробляє їх відповідно до закладених алгоритмів і формує відповідну реакцію.

Алгоритм 1 — Контроль доступу користувачів та пристроїв. Контроль доступу виконується на основі списку дозволених пристроїв (MAC/ID), перевірки ролей користувачів, а також застосування режимів зниженої довіри для підозрілих активностей. Такий механізм дозволяє запобігти несанкціонованим підключенням та обмежити ризик поширення внутрішніх загроз.

Логіка роботи алгоритму контролю доступу полягає в наступному. Спочатку система отримує вхідний запит на підключення, який містить у собі ідентифікатор пристрою (device_id) та роль користувача (user_role). Далі виконується перевірка, чи входить зазначений device_id до переліку дозволених пристроїв. Якщо пристрій дійсно є в цьому списку, здійснюється додаткова перевірка щодо того, чи дозволена відповідна роль користувача для виконання конкретної дії або доступу до певного рівня системи. У разі успішного проходження обох перевірок доступ надається в повному обсязі. Якщо ж пристрій внесено до списку підозрілих або обмежених, активується режим моніторингу із частковим функціоналом, і всі дії користувача журналюються. У випадках, коли пристрій не авторизований і не входить до жодного з визначених списків, система забороняє доступ та фіксує інцидент у журналі безпеки для подальшого аналізу.

Алгоритм 2 — Виявлення аномальної поведінки в подіях. Реалізований алгоритм аналізує вхідні логи подій і сенсорні дані, класифікуючи активність як нормальну або підозрілу. Для цього застосовано методи кластеризації та машинного навчання з бібліотеки scikit-learn, зокрема, алгоритми Isolation Forest і DBSCAN. Вхідними параметрами слугують такі характеристики, як IP-адреса, час запиту, обсяг трафіку, частота доступів та тип виконуваних команд.

Алгоритм функціонує у такий спосіб: спочатку система отримує набір параметрів кожної події в режимі реального часу, включно із часовими мітками, видом операції, ідентифікатором відправника та статистикою за попередній період. Ці параметри порівнюються з історичним профілем звичної поведінки, сформованим у процесі попереднього моніторингу системи. Після цього активується кластеризаційний або деревоподібний алгоритм, що приймає рішення про належність події до «нормального» або «аномального» класу. У разі виявлення аномалії система негайно генерує сигнал тривоги, який передається до підсистеми реагування. Результати аналізу, незалежно від виявленої аномалії, автоматично заносяться до журналу подій, що дає можливість надалі проводити детальні розслідування та коригування поведінкових моделей.

Алгоритм 3 — Шифрування критичних повідомлень. У запропонованій моделі захисту реалізовано механізм симетричного шифрування, що базується на стандартних криптографічних бібліотеках (зокрема, cryptography для Python). Такий підхід дає змогу забезпечити як захист каналу передачі, так і шифрування логів для подальшого безпечного аудиту.

Процес роботи алгоритму передбачає кілька послідовних етапів. На початку сесії або безпосередньо перед передачею даних система генерує криптографічний ключ, який може бути або тимчасовим (одноразовим), або стійким у межах сеансу. Далі отримується вхідне повідомлення — це може бути як телеметричне значення із сенсора, так і команда до виконавчого пристрою. Застосовуючи сформований ключ, алгоритм шифрує це повідомлення за допомогою вибраного криптографічного методу. Після цього зашифрована інформація передається до цільового вузла або зберігається в захищеному журналі. У разі потреби дані можуть бути розшифровані на стороні отримувача з використанням відповідного ключа, що забезпечує цілісність і конфіденційність на всьому шляху обробки.

Розроблені алгоритми були об’єднані в єдину концептуальну модель, яка охоплює всі ключові етапи захисту інформації в автоматизованій системі: від перевірки доступу до реагування на інциденти. Модель побудована на принципах модульності, взаємодії логічно ізольованих компонентів і автоматичного реагування (рис. 2).

Запропонована концептуальна модель інформаційного захисту в автоматизованих системах охоплює повний цикл взаємодії — від автентифікації користувачів і пристроїв

до прийняття рішень щодо реагування на загрози та забезпечення цілісності даних. Вона сформована на основі модульного принципу, що дозволяє гнучко адаптувати її під конкретну архітектуру SCADA, IIoT або MES-середовища. На вході моделі здійснюється збір подій і запитів від сенсорів або користувачів. Першим функціональним блоком виступає модуль автентифікації та контролю доступу, який перевіряє роль користувача (user_role), ідентифікатор пристрою (device_id), застосовує MAC/ID-фільтрацію та аналізує дійсність токена доступу. Якщо запит порушує політики доступу, активується блокування або моніторинговий режим, а подія фіксується в журналі.

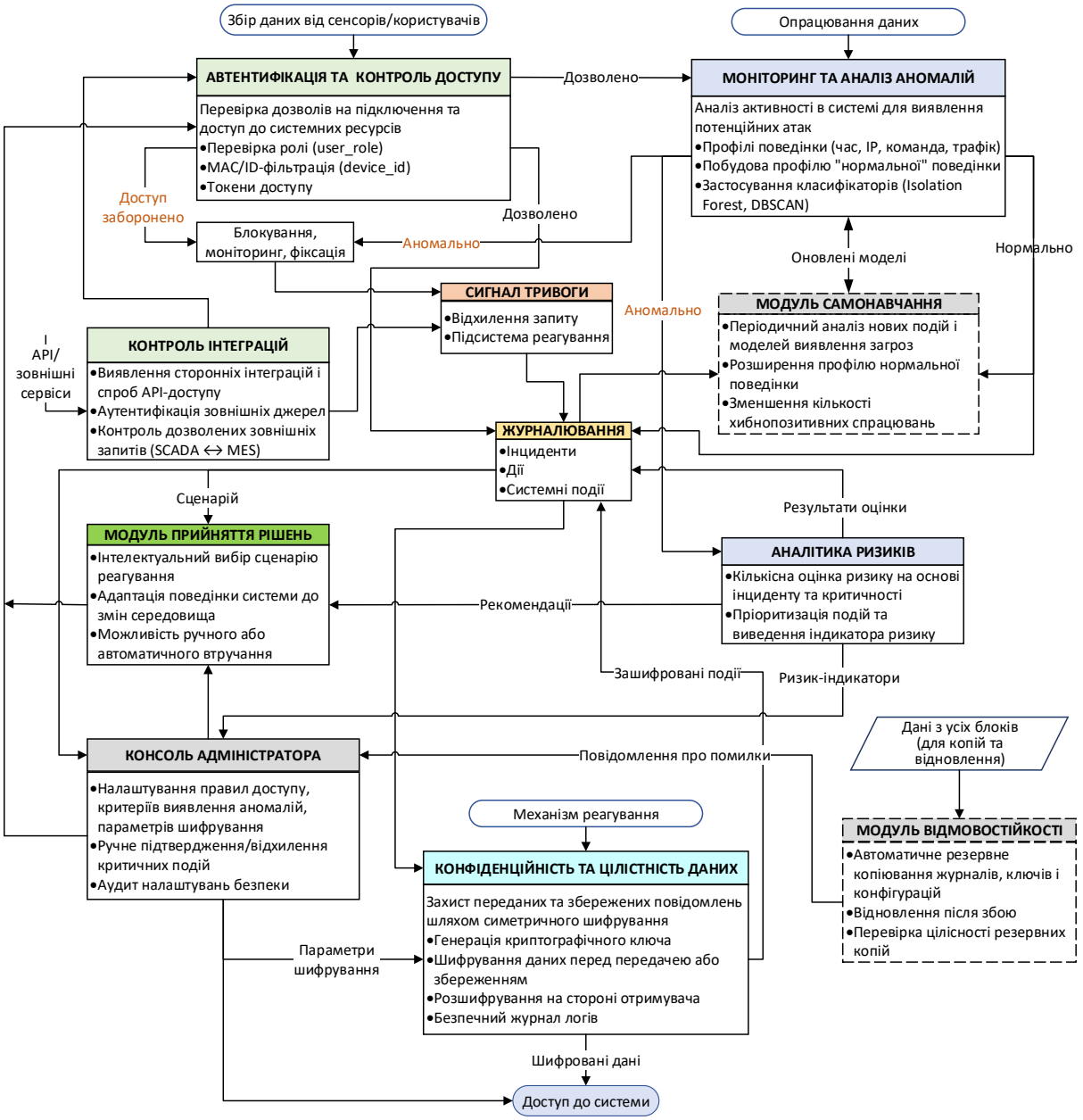

Рис. 2. Концептуальна модель інформаційного захисту в АС

Наступним етапом є моніторинг і аналіз аномалій, де за допомогою алгоритмів кластеризації та машинного навчання (Isolation Forest, DBSCAN) система класифікує дії як нормальні або аномальні. У разі виявлення підозрілої активності формується сигнал тривоги, який передається до блоку прийняття рішень і системи реагування. Паралельно результати аналізу надходять до модуля аналітики ризиків, який виконує кількісну оцінку інциденту на основі його ймовірності та критичності, формує ризик-індикатори та передає їх у блок прийняття рішень. Модуль прийняття рішень реалізує вибір сценарію дій залежно від отриманих ризик-індикаторів та рекомендацій адміністратора. Система може адаптувати свою поведінку до змін у середовищі, автоматично втручатися або очікувати ручного підтвердження. Консоль адміністратора відіграє роль центрального засобу керування політиками безпеки: тут налаштовуються параметри доступу, критерії виявлення загроз, правила шифрування, а також виконується аудит налаштувань. Модуль конфіденційності та цілісності даних забезпечує шифрування критичних повідомлень і логів із використанням симетричних алгоритмів. Він генерує криптографічні ключі, реалізує шифрування/дешифрування даних, контролює журнал безпечного зберігання подій. У випадку збою або компрометації активується модуль відмовостійкості, який відповідає за резервне копіювання налаштувань, перевірку цілісності копій та автоматичне відновлення після збоїв.

Своєрідним захисним бар'єром від зовнішнього впливу є блок контролю інтеграцій, що обробляє запити з API або зовнішніх сервісів. Він виконує автентифікацію джерел, перевіряє допустимість запиту та обмежує неконтрольовану взаємодію, зокрема, між SCADA і MES-рівнями. Додатково реалізовано модуль самонавчання, який оновлює поведінкові моделі, враховує результати аналізу інцидентів і зменшує ймовірність хибнопозитивних спрацювань. Усі дії, незалежно від типу інциденту чи результату, реєструються в модулі журналювання. Це дозволяє системі накопичувати інформацію для наступного аудиту, формування поведінкових шаблонів та вдосконалення моделей реагування. У результаті модель забезпечує не лише виявлення та блокування загроз, але й надає інструменти для формалізованої оцінки ефективності, адаптації до змін і побудови стійкої цифрової інфраструктури.

Для перевірки працездатності концептуальної моделі захисту інформації було реалізовано окремі модулі в середовищі Python 3.10, яке обрано за універсальність та наявність відповідних бібліотек для моделювання, обробки даних і кіберзахисту. Контроль доступу, виявлення аномалій і шифрування реалізовано як модульна система, що дозволяє імітувати події в умовно-захищеній інфраструктурі. Для симетричного шифрування використано бібліотеку cryptography (модуль Fernet). Обробка журналів подій та аналіз трафіку здійснювалися за допомогою pandas. Виявлення аномалій реалізовано з використанням бібліотеки scikit-learn та алгоритмів кластеризації: Isolation Forest, DBSCAN, KMeans. Вхідні параметри включали час доступу, кількість запитів, тип команд і обсяг трафіку, що дозволило ефективно ідентифікувати відхилення в поведінці системи. Усі функціональні модулі були інтегровані у віртуальне захищене середовище, що працювало в режимі реального часу. Це забезпечило можливість адаптивного реагування системи на події: надання або обмеження доступу, шифрування критичних повідомлень, активація режиму моніторингу та збереження інцидентів у журналі для подальшого аналізу.

Для перевірки ефективності розробленої моделі захисту було проведено моделювання типових загроз в автоматизованих системах. Реалізовано низку імітаційних сценаріїв, що відтворювали поширені вектори атак у середовищах SCADA та IIoT: несанкціоноване підключення, підміна даних або команд, аномальна активність,

спроби доступу з заблокованих ID, витоки через незашифровані канали. Події генерувались із заданими параметрами: ID пристрою, IP-адреса, тип операції, роль користувача, частота звернень, і фіксувались у структурованих логах. Сценарії виконувались у двох режимах: до та після активації захисних механізмів. Це дало можливість оцінити реакцію системи, зафіксувати кількість заблокованих запитів, виявлених аномалій та змін у поведінці системи.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для перевірки працездатності концептуальної моделі були реалізовані базові функціональні блоки системи захисту в середовищі Python. Нижче наведено фрагменти коду, які демонструють принцип роботи кожного модуля.

Модуль «Контроль доступу користувачів і пристроїв» забезпечує перевірку ідентифікатора пристрою (наприклад, MAC-адреси або логічного ID) та відповідної ролі користувача. Залежно від встановлених правил система приймає рішення про надання повного доступу, увімкнення режиму моніторингу або повну відмову:

```
# Дозволені пристрої та їх ролі
approved_devices = {'device_01': 'admin', 'device_02': 'operator'}
watchlist = {'device_99'}

def check_access(device_id, role):
    if device_id in approved_devices and approved_devices[device_id] == role:
        return "Доступ дозволено"
    elif device_id in watchlist:
        return "Режим моніторингу"
    else:
        return "Доступ заборонено"

# Приклад виклику:
print(check_access('device_01', 'admin'))  # -> Доступ дозволено
```

Фрагмент коду модуля «Виявлення аномальної поведінки в системі» ілюструє використання алгоритму Isolation Forest з бібліотеки scikit-learn. Цей алгоритм застосовується для виявлення нетипових патернів у поведінці пристроїв або користувачів на основі вхідних параметрів, таких як обсяг трафіку та частота запитів:

```
from sklearn.ensemble import IsolationForest
import numpy as np

# Навчальні дані: середній час доступу, обсяг трафіку
X_train = np.array([[0.2, 100], [0.3, 95], [0.25, 102]])
X_test = np.array([[0.4, 300]])  # Підозрілий трафік

model = IsolationForest()
model.fit(X_train)

if model.predict(X_test)[0] == -1:
    print("Виявлено аномалію")
else:
    print("Активність в межах норми")
```

ISSN 2663 - 4023

Фрагмент коду модуля «Шифрування критичних повідомлень» демонструє використання симетричного шифрування за допомогою бібліотеки cryptography. У модулі реалізовано генерацію ключа, шифрування та дешифрування повідомлення, що дозволяє забезпечити конфіденційність як при передачі, так і при зберіганні даних:

```
from cryptography.fernet import Fernet

# Генерація ключа та шифрування повідомлення
key = Fernet.generate_key()
cipher = Fernet(key)

message = 'Температура: 72.5C'.encode(encoding="utf-8")
encrypted = cipher.encrypt(message)
decrypted = cipher.decrypt(encrypted)

print("Зашифроване:", encrypted)
print("Розшифроване:", decrypted.decode())
```

Інтеграція цих трьох модулів у єдину систему забезпечує адаптивну відповідь на потенційні загрози в автоматизованому середовищі. У процесі перевірки працездатності розробленої концептуальної моделі було реалізовано низку тестових сценаріїв, що імітують найбільш поширені загрози для автоматизованих систем. Для кожного сценарію генерувалися відповідні події, які оброблялися захисними модулями з фіксацією результатів у журналі. Це дозволило оцінити адаптивність моделі до несанкціонованих дій, аномальної поведінки, спроб порушення політик доступу або передачі даних без шифрування. У табл. 2 представлено отримані результати.

Таблиця 2

Результати моделювання типових загроз

№	Тип загрози	Імітована подія / умова	Виклик / фрагмент коду	Реакція системи	Результат
1	Несанкціоноване підключення	`device_id = 'device_77'`, не в approved_devices	`check_access('device_77', 'user')`	Відхилення доступу, запис в log	Заборонено, інцидент зафіксовано
2	Підміна команд	Команда `shutdown()` від `sensor`	`if role != 'admin': deny()`	Роль не відповідає політиці	Відхилено, подія логується
3	Аномальна активність (DoS)	100+ запитів/хвилину від одного IP	`IsolationForest.predict(X_test)`	Виявлена аномалія, генерація тривоги	Аномалія зафіксована
4	Витік/ перехоплення даних	Дані передані без шифрування	`cipher.encrypt(message)`	Активовано шифрування перед передачею	Захищено, інформація передана безпечно
5	Доступ з заблокованого ID	`device_id = 'device_99'` в списку `watchlist`	`check_access('device_99', 'operator')`	Режим моніторингу активовано	Частковий доступ, подія логовано

Після аналізу події або спроби доступу система приймає рішення про шифрування, блокування або подальший моніторинг, забезпечуючи баланс між безпекою та продуктивністю. У рамках дослідження були обчислені три ключові коефіцієнти: ризику, ефективності виявлення атак та ентропії розподілу доступу.

Коефіцієнт ризику (R) — показник, що визначає рівень потенційної загрози з урахуванням імовірності події та рівня її впливу. Він розраховується за формулою:

$$R = P \cdot I, \quad (1)$$

де P — імовірність реалізації загрози, I — ступінь впливу (шкала від 1 до 10).

Ефективність виявлення атак (E) — оцінює здатність системи виявляти аномальні події вчасно. Формула враховує кількість виявлених атак та середній час реакції:

$$E = \frac{N_{\text{виявлено}}}{T_{\text{реакції}} \cdot N_{\text{загалом}}}, \quad (2)$$

де $N_{виявлено}$ — кількість атак, виявлених системою, $N_{загалом}$ — загальна кількість атак, $T_{реакції}$ — середній час реакції в секундах.

Ентропія розподілу доступу (H) – показник, що характеризує рівень випадковості або нерегулярності в розподілі доступів. Ентропія розраховується за формулою Шеннона:

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i, \quad (3)$$

де p_i — ймовірність вибору певної ролі/доступу серед усіх. Чим вища ентропія, тим більш розподілені та захищені ролі в системі.

Отримані результати моделювання (табл. 3) свідчать про підвищення ефективності реагування системи після інтеграції запропонованої концептуальної моделі. Спостерігається зменшення ризику більш ніж на 50%, зростання точності виявлення атак і більш збалансований розподіл прав доступу, що підтверджується зростанням ентропії.

Таблиця 3

Порівняння показників ефективності системи до й після впровадження моделі

Тип загрози	Коефіцієнт ризику R		Виявлення атак (%)		Середній час реакції (сек.)		Ентропія доступу H	
	до	після	до	після	до	після	до	після
Несанкціоноване підключення	4.5	1.1	0	98	7.5	2.5	0.72	1.45
Підміна команд	4.8	1.2	0	95	6.8	2.2	0.65	1.42
Аномальна активність (DoS)	5.2	1.4	20	93	9.2	3.1	0.70	1.38
Витік/перехоплення даних	4.9	1.3	0	97	8.5	2.7	0.68	1.40
Спроба доступу з заблокованого ID	3.7	1.0	10	96	7.0	2.0	0.60	1.44

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Більшість сучасних рішень із кібербезпеки в автоматизованих системах зосереджуються на окремих задачах, зокрема, автентифікації, виявленні аномалій або шифруванні без побудови повноцінного захисного контуру. Така фрагментарність знижує ефективність у складних інфраструктурах, особливо в умовах зростання кіберзагроз. На відміну від них, запропонована концептуальна модель інтегрує три ключові механізми: контроль доступу, виявлення аномалій та шифрування критичних повідомлень. Вона реалізована у вигляді модульної системи та передбачає формалізовану оцінку ефективності за кількісними метриками, що забезпечує цілісне

реагування на загрози й робить модель придатною для практичного впровадження в промислових АС.

Запропонована модель має гнучку модульну архітектуру, що включає механізми контролю доступу, виявлення аномалій та шифрування. Кожен компонент функціонує незалежно, що дозволяє адаптувати систему до специфіки підприємства без зміни загальної логіки. Реалізація на базі Python і відкритих бібліотек забезпечує доступність та простоту впровадження, навіть у середовищах з обмеженими ресурсами. Формалізовані метрики (коефіцієнт ризику, точність виявлення, ентропія доступу) дають змогу кількісно оцінювати ефективність захисту та коригувати політики безпеки. Модель підтримує поетапне впровадження: від базової перевірки доступу до повноцінного захисту даних. Завдяки універсальній структурі її можна масштабувати: на edge-пристроях в IoT, у шлюзах SCADA або в хмарних рішеннях для смарт-виробництва. Це робить модель сумісною з різними протоколами та ефективною в умовах складних цифрових інфраструктур.

У процесі дослідження було розроблено та реалізовано концептуальну модель захисту інформації в автоматизованих системах, що поєднує три основні напрямки: контроль доступу, виявлення аномальної активності та шифрування критичних повідомлень. Усі механізми організовано у вигляді логічно взаємопов’язаних модулів із чітко визначеною архітектурою та алгоритмічною структурою. Запропонована модель не лише забезпечує багаторівневий захист, а й дозволяє формалізовано оцінити ефективність впроваджених заходів. Це створює умови для прийняття обґрунтованих рішень щодо удосконалення інформаційної безпеки в АС.

Практична цінність моделі полягає в її гнучкості, доступності та можливості масштабування. Реалізація на основі відкритого програмного забезпечення дозволяє застосовувати її як у малих підприємствах і навчальних симуляторах, так і в складних промислових системах SCADA та IoT. У перспективі передбачається інтеграція самонавчальних механізмів для адаптації до змін середовища, застосування штучного інтелекту для прогнозування атак та розгортання моделі в реальних виробничих умовах. Отже, запропоноване рішення формує основу для створення адаптивних і стійких систем захисту, здатних ефективно протистояти актуальним кіберзагрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mazurenko, V. B., et al. (2021). Osnovni zakhody zabezpechennia kiberbezpeky suchasnykh system promyslovoi avtomatyzatsii. *Actual problems of automation and information technology*, *25*, 108–118. https://doi.org/10.15421/432112
2. Panovyk, U. P. (2024). Kiberbezpeka v telekomunikatsiinykh merezhakh ta systemakh. *Naukovi zapysky, 1(68)*, 122–135. https://doi.org/10.32403/1998-6912-2024-1-68-122-135
3. Chepel, L. V., & Boiko, Yu. V. (2024). Pidkhid do bezpeky ta orhanizatsii merezh IoT z vykorystanniam blokchein tekhnolohii. *Visnyk VPI, 175(4),* 129–138. https://doi.org/10.31649/1997-9266-2024-175-4-129-138
4. AL-Hawawreh, M., & Sitnikova, E. (2020). Developing a Security Testbed for Industrial Internet of Things. *IEEE Internet of Things Journal*. *8(7),* 5558–5573. https://doi.org/10.1109/jiot.2020.3032093
5. Aouedi, O., et al. (2024). A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions. *IEEE Communications Surveys & Tutorials*, 27(2), 1238–1292. https://doi.org/10.1109/comst.2024.3430368
6. Barsha N. K., & Hubballi N. (2024). Anomaly Detection in SCADA Systems: A State Transition Modeling. *IEEE Transactions on Network and Service Management, 21(3),* 3511–3521. https://doi.org/10.1109/tnsm.2024.3373881

7. Chih-Yuan Lin. (2020). A timing approach to network-based anomaly detection for SCADA systems. *Linköping: Linköping University Electronic Press.* https://doi.org/10.3384/lic.diva-165155
8. Hassan ALI, et al. (2023). Cellsecure: Securing image data in industrial internet-of-things via cellular automata and chaos-based encryption. *In 2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*, 1–6. https://arxiv.org/abs/2309.11476
9. MES and Security. *Critical Manufacturing*. (n. d.). https://www.criticalmanufacturing.com/blog/mes-and-security/?utm_source=chatgpt.com
10. MES Computing's 10 Most-Viewed Stories In 2024. (2024). *MES Computing - Daily Technology News for Midmarket IT Leaders*. https://www.mescomputing.com/news/business/mes-computing-s-10-most-viewed-stories-in-2024?utm_source=chatgpt.com
11. Mosteiro-Sanchez, A., et al. (2020). Securing IIoT using Defence-in-Depth: Towards an End-to-End secure Industry 4.0. *Journal of Manufacturing Systems*, 57, 367–378. https://doi.org/10.1016/j.jmsy.2020.10.011
12. Motakatla Venkateswara Reddy, et al. (2023). Cybersecurity Anomaly Detection in SCADA-Assisted OT Networks Using Ensemble-Based State Prediction Model. *U.S. Department of Energy Office of Scientific and Technical Information*. https://doi.org/10.2172/1996392
13. Okur C., & Dener M. (2025). Symmetrical Resilience: Detection of Cyberattacks for SCADA Systems Used in IIoT in Big Data Environments. *Symmetry*, *17(4):480*. https://doi.org/10.3390/sym17040480
14. Phillips, B., Gamess, E. & Krishnaprasad, S. (2020). An Evaluation of Machine Learning-based Anomaly Detection in a SCADA System Using the Modbus Protocol. *Conference: ACM Southeast Conference At: Tampa, FL, USA*. https://doi.org/10.1145/3374135.3385282
15. Poorazad, S. K., Benzaïd, C. & Taleb, T. (2023). Blockchain and deep learning-based ids for securing sdn-enabled industrial iot environments. *In GLOBECOM 2023-2023 IEEE Global Communications Conference*, 2760–2765. https://arxiv.org/abs/2401.00468
16. Shaporin, V. O., Tishin, P. M., & Shaporina, O. L. (2018). Vulnerability ontology in SCADA systems. *Systems and Technologies*, *1(56)*, 18–29. https://doi.org/10.32836/2521-6643-2018-1-56-2
17. Shulika, K. et al. (2024). A method of using modern endpoint detection and response (EDR) systems to protect against complex attacks. *Innovative technologies and scientific solutions for industries*, *2(28)*, 182–195. https://doi.org/10.30837/2522-9818.2024.2.182

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Ulyana Panovyk
PhD, Associate Professor,
Associate Professor of the Department of Computer Technologies in Publishing and Printing Processes,
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-9663-4328
uliana.p.panovyk@lpnu.ua

INFORMATION PROTECTION IN AUTOMATED SYSTEMS BASED ON A CONCEPTUAL MODEL WITH FORMALIZED EFFICIENCY EVALUATION

Abstract. In the context of increasing cyber threats and the implementation of digital technologies in production process management, automated systems are increasingly becoming targets of attacks, raising the issue of ensuring information security at critical levels. This is particularly relevant for SCADA, IIoT, and MES environments, where the use of isolated solutions without a unified security architecture leads to vulnerabilities and reduced effectiveness in incident response. The article presents a conceptual model of information protection that integrates access control, anomaly detection, and encryption of critical messages, and includes a formalized evaluation of effectiveness based on quantitative metrics. The methodological foundation of the study involves structural threat modeling, algorithmic design of protective mechanisms, implementation of functional modules in the Python environment, and simulation of behavioral scenarios using generated event logs. To assess the effectiveness of the security model, metrics such as risk coefficient, detection rate, access entropy, and average response time were used. The algorithms operate in real time, responding to events according to a predefined logic: the system blocks or limits suspicious actions, activates encryption of critical messages, and logs all incidents in the event journal. The simulation confirmed the effectiveness of the proposed model: the risk coefficient was reduced by more than half, the attack detection accuracy reached 95–98%, and the access entropy increased, indicating a more balanced and secure rights management. The proposed model establishes a multi-level security architecture that can be implemented in both traditional SCADA and MES systems, as well as IIoT infrastructures. Thanks to its flexible structure, open implementation, and adaptability, the model can be scaled to meet specific enterprise needs and applied in resource-constrained environments or large industrial systems. The obtained results demonstrate the practical applicability of the model for ensuring reliable data protection in the modern cyber environment.

Keywords: automated systems; information security; SCADA; IIoT; access control; anomaly detection; encryption; conceptual model; security effectiveness.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Mazurenko, V. B., et al. (2021). Osnovni zakhody zabezpechennia kiberbezpeky suchasnykh system promyslovoi avtomatyzatsii. *Actual problems of automation and information technology*, *25*, 108–118. https://doi.org/10.15421/432112
2. Panovyk, U. P. (2024). Kiberbezpeka v telekomunikatsiinykh merezhakh ta systemakh. *Naukovi zapysky, 1(68),* 122–135. https://doi.org/10.32403/1998-6912-2024-1-68-122-135
3. Chepel, L. V., & Boiko, Yu. V. (2024). Pidkhid do bezpeky ta orhanizatsii merezh IoT z vykorystanniam blokchein tekhnolohii. *Visnyk VPI, 175(4),* 129–138. https://doi.org/10.31649/1997-9266-2024-175-4-129-138
4. AL-Hawawreh, M., & Sitnikova, E. (2020). Developing a Security Testbed for Industrial Internet of Things. *IEEE Internet of Things Journal*. *8(7),* 5558–5573. https://doi.org/10.1109/jiot.2020.3032093
5. Aouedi, O., et al. (2024). A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions. *IEEE Communications Surveys & Tutorials*, 27(2), 1238–1292. https://doi.org/10.1109/comst.2024.3430368
6. Barsha N. K., & Hubballi N. (2024). Anomaly Detection in SCADA Systems: A State Transition Modeling. *IEEE Transactions on Network and Service Management, 21(3),* 3511–3521. https://doi.org/10.1109/tnsm.2024.3373881

7. Chih-Yuan Lin. (2020). A timing approach to network-based anomaly detection for SCADA systems. *Linköping: Linköping University Electronic Press.* https://doi.org/10.3384/lic.diva-165155
8. Hassan ALI, et al. (2023). Cellsecure: Securing image data in industrial internet-of-things via cellular automata and chaos-based encryption. *In 2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*, 1–6. https://arxiv.org/abs/2309.11476
9. MES and Security. *Critical Manufacturing*. (n. d.). https://www.criticalmanufacturing.com/blog/mes-and-security/?utm_source=chatgpt.com
10. MES Computing's 10 Most-Viewed Stories In 2024. (2024). *MES Computing - Daily Technology News for Midmarket IT Leaders*. https://www.mescomputing.com/news/business/mes-computing-s-10-most-viewed-stories-in-2024?utm_source=chatgpt.com
11. Mosteiro-Sanchez, A., et al. (2020). Securing IIoT using Defence-in-Depth: Towards an End-to-End secure Industry 4.0. *Journal of Manufacturing Systems*, 57, 367–378. https://doi.org/10.1016/j.jmsy.2020.10.011
12. Motakatla Venkateswara Reddy, et al. (2023). Cybersecurity Anomaly Detection in SCADA-Assisted OT Networks Using Ensemble-Based State Prediction Model. *U.S. Department of Energy Office of Scientific and Technical Information*. https://doi.org/10.2172/1996392
13. Okur C., & Dener M. (2025). Symmetrical Resilience: Detection of Cyberattacks for SCADA Systems Used in IIoT in Big Data Environments. *Symmetry*, *17(4):480*. https://doi.org/10.3390/sym17040480
14. Phillips, B., Gamess, E. & Krishnaprasad, S. (2020). An Evaluation of Machine Learning-based Anomaly Detection in a SCADA System Using the Modbus Protocol. *Conference: ACM Southeast Conference At: Tampa, FL, USA*. https://doi.org/10.1145/3374135.3385282
15. Poorazad, S. K., Benzaïd, C. & Taleb, T. (2023). Blockchain and deep learning-based ids for securing sdn-enabled industrial iot environments. *In GLOBECOM 2023-2023 IEEE Global Communications Conference*, 2760–2765. https://arxiv.org/abs/2401.00468
16. Shaporin, V. O., Tishin, P. M., & Shaporina, O. L. (2018). Vulnerability ontology in SCADA systems. *Systems and Technologies*, *1(56)*, 18–29. https://doi.org/10.32836/2521-6643-2018-1-56-2
17. Shulika, K. et al. (2024). A method of using modern endpoint detection and response (EDR) systems to protect against complex attacks. *Innovative technologies and scientific solutions for industries*, *2(28)*, 182–195. https://doi.org/10.30837/2522-9818.2024.2.182