УДК 004.056.5:004.896:004.7.056
DOI: 10.31673/2409-7292.2026.011827

Яковенко В.О., Мормуль М.Ф.

ПРОЄКТУВАННЯ КІБЕРЗАХИСТУ ЕЛЕКТРОННИХ СЕРВІСІВ У ПРОЦЕСІ РЕІНЖИНІРИНГУ: НУЛЬОВА ДОВІРА, ПОДІЄВА АНАЛІТИКА ТА ДЕТЕКЦІЯ ПРОШИВКОВИХ І МЕРЕЖЕВИХ АТАК МЕТОДАМИ ГЛИБОКОГО НАВЧАННЯ

У роботі запропоновано цільову архітектуру кіберзахисту електронних послуг у процесі реінжинірингу яка поєднує підхід нульової довіри, подієвий контур моніторингу на основі системи виявлення вторгнень і системи керування інформацією та подіями безпеки, а також модулі виявлення аномалій на основі глибокого навчання. Актуальність зумовлена гібридними кібератаками, де мережеві експлойти поєднуються з модифікацією вбудованого програмного забезпечення в ланцюгах постачання та оновлення і з експлуатацією слабкостей протоколу захищеного транспортного рівня та простого протоколу керування мережею у вбудованих пристроях. Мета полягає в інтеграції безпеки рівня підприємства в архітектуру послуг і підтвердженні детекції та реагування за часом до виявлення, часом до пом'якшення наслідків і частками хибних спрацювань. Запропоновано дворівневу кореляцію: детерміновані правила для індикаторів компрометації та корелятор машинного навчання для прихованих залежностей між подіями. Для часових послідовностей використано автокодер з рекурентною нейронною мережею довгої короткочасної пам'яті, де реконструкційна помилка є мірою аномальності. Для бінарних і пакетних структур застосовано перетворення байтових послідовностей у зображення та зв'язку згорткової нейронної мережі з рекурентною нейронною мережею довгої короткочасної пам'яті. Моделювання охоплює зниження версії захищеного з'єднання, помилки перевірки сертифікатів, компрометацію рядків спільноти керувального протоколу і доступ на запис, а також ін'єкцію модифікованих прошивок у канали оновлень. Показано скорочення часу до виявлення та зменшення шуму інцидентів порівняно з підходом, що спирається лише на сигнатури. Практична цінність полягає в патернах політик взаємної автентифікації сервісів, інфраструктури відкритих ключів, принципі мінімальних привілеїв і контрольних точках у ланцюгах оновлення прошивок та налаштуваннях протоколів.

Ключові слова: підхід нульової довіри, система виявлення вторгнень, система керування інформацією та подіями безпеки, протокол захищеного транспортного рівня, простий протокол керування мережею, вбудоване програмне забезпечення, перетворення байтових послідовностей у зображення, згорткова нейронна мережа, рекурентна нейронна мережа довгої короткочасної пам'яті, автокодер, кореляція подій безпеки.

Вступ

Реінжиніринг електронних послуг у державному та корпоративному секторі майже завжди завершується переходом до цільової архітектури майбутнього стану (TO-BE), у якій домінують мікросервісні компоненти, шлюзи прикладних інтерфейсів, контейнерні середовища, хмарні та гібридні інтеграції, а також розподілене адміністрування. У такій екосистемі класичний «периметр» безпеки втрачає визначеність: транзакції проходять крізь множину сервісів, залежностей і доменів довіри, а компрометація одного вузла може запускати ланцюгові наслідки. Це відповідає загальному зсуву від традиційного «захисту інформації» до ширшого поняття кібербезпеки, де ключову роль відіграють взаємозалежності компонентів і процесів на рівні підприємства [1].Додатковий чинник ризику створює поширення вбудованих мережевих пристроїв і керованих компонентів інфраструктури, у яких уразливості конфігурації та реалізацій здатні існувати роками, а їх експлуатація часто маскується під легітимні адміністративні дії. Широкомасштабні спостереження щодо небезпечності вбудованих мережевих пристроїв підтверджують, що саме цей клас активів є одним із найуразливіших сегментів сучасних мереж [10]. У контексті електронних послуг це підсилюється ризиками ланцюга постачання та оновлення вбудованого програмного забезпечення: навіть «незначна» модифікація прошивки може змінити мережеву поведінку, політики шифрування або керувальні команди так, що відхилення виглядатимуть як нормальна робота сервісу.Стратегічною відповіддю на зникнення чітких меж довіри у мікросервісних і гібридних середовищах є модель нульової довіри (Zero Trust), яка формалізує принцип: жоден суб'єкт, пристрій або сервіс не є довіреним за замовчуванням, а доступ має надаватися за контекстом, політиками та безперервною перевіркою [6]. Для кіберфізичних і розподілених систем важливими є також патерни проєктування й забезпечення нульової

довіри, що підкреслюють необхідність мікросегментації, контролю ідентичностей і керованого прийняття рішень авторизації [14]. При цьому організаційна «рамка» цілей, метрик і керування ризиками узгоджується з практиками фреймворку кібербезпеки, орієнтованого на безперервне вдосконалення та вимірюваність контролів [7]

Окрему практично значущу групу загроз формують уразливості протоколів захищеного транспортного рівня та простого протоколу керування мережею, які в реальних середовищах часто експлуатуються через помилки налаштувань, слабкі параметри сумісності, некоректні реалізації у вбудованих стосах та помилки процесів адміністрування. У прошивкових ланцюгах ці проблеми мають мультиплікативний ефект: змінена прошивка здатна «легально» впливати на параметри захищених сесій або на керувальні команди, і це ускладнює виявлення без контекстної кореляції та профілювання поведінки [10].Для забезпечення детекції та реагування рівня підприємства необхідний подієвий контур моніторингу, у якому датчики мережевого та хостового рівнів збирають сигнали, а механізми керування журналами забезпечують нормалізацію, збагачення та подальшу аналітику. Базові принципи побудови систем виявлення вторгнень та запобігання вторгненням, включно з рекомендаціями щодо збору й інтерпретації телеметрії, узагальнено у профільних настановах [12]. Проте для сучасних гібридних атак недостатньо ізольованих сигнатурних спрацювань: потрібна кореляція різнорідних подій і ланцюгів, що посилює роль систем керування подіями безпеки та кореляційних механізмів, орієнтованих на багатошарові сценарії [15].

Додатково, коли електронні послуги є частиною більш широких цифрових екосистем (наприклад, «цифрових двійників» організаційних процесів або інфраструктури), підвищуються вимоги до узгодження кіберзахисту з моделями системної взаємодії та спостереження [8, 9].Обмеження детермінованої, суто правилової кореляції полягає в тому, що нові тактики та «повільні» багатокрокові атаки часто не мають стабільного сигнатурного профілю. Тому доцільним є гібридний підхід, у якому правила формують керований «каркас» контролю політик, а моделі машинного навчання підсилюють виявлення прихованих залежностей у часових послідовностях і в багатомодальних даних. Для часових послідовностей подій ефективними є рекурентні моделі, зокрема підходи на основі довгої короткочасної пам’яті для виявлення аномалій у потоках подій та великих даних [4], а також варіанти кодувальник–декодувальник для багатосенсорних рядів [5].

Для мережевого трафіку релевантними є моделі типу згорткова мережа плюс рекурентна мережа, які поєднують просторові та часові залежності для аномалій у веб- і мережевих потоках [13].У випадках, коли аналізуються структуровані бінарні артефакти або стабільні «вікна» пакетних даних (зокрема під час контролю прошивок або пов’язаних із ними компонентів), практичним є перетворення байтових послідовностей у зображення (Byte2Image) і подальша класифікація за допомогою нейронних мереж, що добре зарекомендувало себе для виявлення відмінностей у шкідливих і модифікованих бінарних об’єктах [3].

Для виявлення аномалій у програмно визначених мережах та мережах інтернету речей запропоновано гібридні моделі згорткової і рекурентної нейронних мереж, які є релевантними для багатоджерельних, шумних середовищ і можуть використовуватися як аналітичне «підсилення» подієвої кореляції [16, 17]. З огляду на необхідність одночасно досягати швидкості реагування, низької частки хибних спрацювань і достатнього покриття сценаріїв, задача проєктування архітектури кіберзахисту фактично набуває рис багатокритеріальної оптимізації (баланс безпеки, вартості й операційних ресурсів), що узгоджується з класичними підходами до багатокритеріальних методів [2].

Окремо підкреслюється потреба у вимірюваності й відтворюваності: оцінка ефективності має спиратися не лише на метрики моделей, а й на процесні показники центру операцій безпеки, що може бути формалізовано через підходи до процесного аналізу та «процесного майнінгу» для цифрових слідів подій [11].

Постановка проблеми

Сучасний реінжиніринг електронних послуг у державному та корпоративному секторах супроводжується переходом до складних архітектур майбутнього стану (TO-BE), що базуються на мікросервісах, контейнеризації та гібридних хмарних інтеграціях. У таких екосистемах класичний захисний «периметр» втрачає свою визначеність, оскільки транзакції проходять крізь множину доменів довіри, а компрометація навіть одного вузла може спричинити каскадні наслідки для всієї системи.

Додатковий критичний чинник ризику створює поширення вбудованих мережевих пристроїв, уразливості яких можуть існувати роками, а їхня експлуатація часто маскується під легітимні адміністративні дії. Особливу небезпеку становлять гібридні атаки, що поєднують мережеві експлойти з модифікацією вбудованого програмного забезпечення (прошивок) у ланцюгах постачання, що дозволяє зловмисникам змінювати поведінку сервісів, залишаючись непоміченими для традиційних засобів захисту. Отже, виникає гостра потреба у проєктуванні нових архітектур кіберзахисту, які б забезпечували безперервну перевірку кожного суб'єкта та глибоку аналітику подій для виявлення складних аномалій.

Аналіз останніх досліджень і публікацій

Фундаментом для побудови сучасних систем захисту є модель нульової довіри (Zero Trust), принципи якої формалізовані у стандарті NIST SP 800-207. Дослідження патернів проєктування нульової довіри для розподілених та кіберфізичних систем підкреслюють важливість мікросегментації та динамічного управління ідентичностями. Організаційна рамка управління ризиками та вимірюваності контролів узгоджується з фреймворком NIST CSF 2.0.

Для детекції загроз традиційно використовуються системи виявлення вторгнень (IDS) та засоби керування подіями безпеки (SIEM), що спираються на сигнатурний аналіз та детерміновані правила кореляції. Проте для протидії багатошаровим атакам все частіше застосовуються методи глибокого навчання:

1. Рекурентні нейронні мережі (LSTM) ефективно виявляють аномалії у часових послідовностях подій та великих даних;

2. Гібридні моделі, що поєднують згорткові (CNN) та рекурентні мережі, демонструють високу якість аналізу мережевого трафіку в середовищах SDN та IoT;

3. Підхід перетворення байтових послідовностей у зображення (Byte2Image) дозволяє візуалізувати та класифікувати модифіковані бінарні об'єкти й шкідливе ПЗ.

Водночас питання інтеграції цих методів у єдиний подієвий контур моніторингу в процесі реінжинірингу е-послуг, з урахуванням специфіки прошивкових атак та операційних метрик реагування (TTD/TTM), потребує подальшого дослідження.

Завдання дослідження

Метою роботи є обґрунтування та практична реалізація способу вбудування захисту рівня підприємства в архітектуру електронних послуг. Для досягнення цієї мети визначено такі завдання:

1. Спроєктувати контур нульової довіри, що базується на мікросегментації, контролі ідентичностей та суворих політиках доступу;

2. Побудувати подієвий контур моніторингу, який забезпечує збір телеметрії з різних датчиків та багаторівневу кореляцію подій;

3. Інтегрувати поведінкові моделі на основі нейронних мереж для виявлення аномалій у часових послідовностях та мережевих потоках;

4. Застосувати аналіз бінарних артефактів за допомогою методу Byte2Image для детекції втручань у прошивки вбудованих пристроїв;

5. Оцінити ефективність запропонованих рішень за допомогою операційних метрик центру операцій безпеки (SOC), таких як час до виявлення та час до пом'якшення наслідків.

Мета роботи полягає у тому, щоб обґрунтувати та показати практичний спосіб вбудування захисту рівня підприємства в цільову архітектуру електронних послуг і

підтвердити ефективність детекції та реагування на гібридні кібератаки, включно з прошивковими векторами та експлуатацією слабкостей протоколів захищеного транспортного рівня і мережевого керування. Для досягнення мети визначено такі завдання: (1) спроєктувати контур нульової довіри з мікросегментацією, контролем ідентичностей та політиками доступу [6, 14, 7]; (2) побудувати подієвий контур моніторингу з датчиками виявлення вторгнень і кореляцією подій [12, 15]; (3) інтегрувати поведінкові моделі виявлення аномалій для часових послідовностей і мережевих потоків [4, 5, 13]; (4) застосувати аналіз бінарних артефактів із використанням перетворення байтів у зображення та гібридних нейромережевих детекторів для сценаріїв, пов'язаних із прошивками та інтернетом речей [3, 16, 17]; (5) забезпечити вимірюваність ефекту та відтворюваність експериментів з урахуванням багатокритеріального характеру компромісів і процесної оцінки реагування [2, 11].

Виклад основного матеріалу дослідження

У цьому розділі подано методи проєктування та експериментальної верифікації запропонованої цільової архітектури кіберзахисту електронних послуг у процесі реінжинірингу. Методологія спирається на розуміння переходу від класичного «захисту інформації» до кібербезпеки як системної властивості взаємопов'язаних сервісів, мереж і процесів [1], а також враховує підвищені ризики, пов'язані з вбудованими мережевими пристроями й їх керованими площинами [10]. Архітектурна частина методів базується на підході нульової довіри, який формалізує безперервну перевірку, мікросегментацію, контроль ідентичностей і керування політиками доступу [6], з урахуванням патернів проєктування та гарантування нульової довіри для розподілених і кіберфізичних середовищ [14]. Узгодження цілей, контролів і вимірюваності виконується в логіці фреймворку кібербезпеки, орієнтованого на керування ризиком і метрики зрілості [7].Експериментальна частина методів організована як сценарійне моделювання для гібридних атак у середовищі електронних послуг, де відтворюються мережеві, керувальні та прошивкові прояви інцидентів. Для збору та інтерпретації телеметрії застосовано підхід «датчики – нормалізація – кореляція», узгоджений з настановами щодо систем виявлення та запобігання вторгненням [12]. Подієва кореляція реалізується як поєднання детермінованих правил та статистично-аналітичного шару, що відповідає сучасним підходам до побудови кореляційних механізмів для багатошарових атак [15].

Для підвищення відтворюваності та формалізації ланцюгів подій у часі додатково застосовано процесний аналіз цифрових слідів, який дозволяє відновлювати типові траєкторії інцидентів і вимірювати операційні затримки реагування [11].Модулі інтелектуальної детекції в методах розглядаються як «підсилювач» подієвого контуру, а не як заміна правил. Для послідовностей подій використано рекурентні моделі для виявлення аномалій у потоках даних [4] та кодувальник–декодувальник для багатосенсорних рядів з реконструкційним критерієм [5]. Для мережевого трафіку як джерела аномалій враховано ефективність гібридних згортково-рекурентних підходів у задачах виявлення нетипової поведінки [13]. Для аналізу структурованих бінарних артефактів і повторюваних «байтових вікон» використано підхід перетворення байтових послідовностей у зображення, що має підтверджену придатність для класифікації модифікованих бінарних об'єктів [3]. Для сценаріїв, близьких до мереж програмно-визначеної архітектури та інтернету речей, застосовність гібридних згортково-рекурентних детекторів розглядається з опорою на профільні дослідження [16, 17]. Окремо методи враховують, що електронні послуги дедалі частіше функціонують у зв'язку з моделями «цифрових двійників» процесів та інфраструктури, де зростає цінність кореляції подій і станів системи на рівні підприємства [8, 9].Оцінювання ефективності методів виконується як багатокритеріальне порівняння архітектурних варіантів (керованість політик, покриття сценаріїв, операційна ефективність реагування, навантаження на команду), що узгоджується з підходами до багатокритеріальної оптимізації [2]. Таким чином, розділ «Методи» формалізує: (1) архітектурні правила побудови нульової довіри; (2) подієвий контур моніторингу і

кореляції; (3) процедури формування наборів даних і сценаріїв; (4) моделі детекції аномалій для різних типів даних; (5) критерії та порядок оцінювання результатів у термінах операційної ефективності й якості аналітики.

TO-BE контур Zero Trust для е-послуг

Запропонована TO-BE архітектура розділяє систему на домени (користувацький, сервісний, даних, керування) і впроваджує мікросегментацію на рівні мережі та сервісів. Доступ надається лише після явної перевірки: (i) ідентичності суб'єкта (користувач/сервіс/пристрій), (ii) дозволів (політики), (iii) стану середовища (постура, ризик), (iv) контексту транзакції [1, 4]. Для міжсервісної взаємодії застосовується mTLS, керування сертифікатами здійснюється через PKI з автоматизацією ротації та відкликання. Адміністрування переводиться на принципи JIT (just-in-time доступ) та JEA (just-enough-administration), що зменшує «вікно» зловживань привілеями.

Політика доступу до API формалізується як задача вибору мінімального набору привілеїв для ролі r за умов покриття необхідних операцій O_r і обмежень ризику B:

$$\min_{\pi_r \subseteq \Pi} |\pi_r| \quad \text{заумов} \quad O_r \subseteq f(\pi_r), \quad \mathcal{R}(\pi_r) \leq B \,, \tag{1}$$

де П – універсум дозволів, $f(\cdot)$ – відображення «дозволи → операції», $\mathcal{R}(\pi_r)$ – ризик, оцінений за контекстними факторами (критичність сервісу, зона сегментації, довіра до пристрою, історія інцидентів). Практично $\mathcal{R}(\cdot)$ може бути агрегатом з CVSS-похідних оцінок активів і поточного рівня загроз, що підтримує керованість ризику при розширенні системи [22, 2].

Подієвий контур моніторингу є «нервовою системою» цільової архітектури кіберзахисту електронних послуг: саме він перетворює розрізнені технічні сигнали (мережеві спостереження, журнали сервісів, адміністративні дії та телеметрію оновлень) на керовані інциденти з пріоритетами, причинами та рекомендованими діями. У мікросервісних і гібридних середовищах одиничний сигнал майже ніколи не дає повної картини, тому ключовим стає нормалізований збір подій та кореляція на рівні системи керування інформацією та подіями безпеки, що дозволяє пов'язувати порушення політик доступу, аномалії поведінки та ознаки компрометації в єдиний ланцюг. Такий підхід відповідає практикам побудови систем виявлення та запобігання вторгненням і вимогам до вимірюваного реагування (скорочення часу до виявлення та часу до пом'якшення наслідків) [12, 15].У межах цієї роботи подієвий контур реалізовано як багатоджерельну схему «датчики → нормалізація → кореляція → оркестрація реагування». На вході використовуються мережеві датчики та хостові агенти, журнали прикладних інтерфейсів і шлюзів, а також події керування вбудованим програмним забезпеченням і мережевими параметрами, включно з керувальними протоколами. Далі застосовується узгоджена нормалізація полів події (час, джерело/призначення, сервіс, дія, результат, контекст активу та атрибути протоколів), після чого кореляція виконується дворівнево: детермінованими правилами для фіксації порушень політик і статистично-аналітичним корелятором для виявлення прихованих залежностей у часових послідовностях і між сенсорами [13-15]. На виході формується тригер для плейбуків реагування (оркестрація та автоматизація), а ефект контролюється показниками операційної ефективності центру операцій безпеки [15, 21].

Рисунок 1 ілюструє подієво-орієнтовану архітектуру кіберзахисту електронних послуг, у якій дані з кількох джерел зводяться до спільного формату та корелюються для виявлення гібридних атак. У верхній частині показані джерела подій: (1) мережеві датчики (спостереження потоків і глибший аналіз трафіку), (2) хостові агенти (журнали операційних систем і телеметрія засобів захисту кінцевих точок), (3) журнали шлюзу прикладних інтерфейсів (виклики, автентифікація, помилки, політики доступу), (4) події прошивок і мережевого керування (оновлення, конфігурації, керувальні команди). Ці потоки сходяться в шар нормалізації подій, де кожній події надається єдина структура (часова мітка,

джерело/призначення, сервіс, дія, результат і набір атрибутів, зокрема параметри захищеного з'єднання та керувальних операцій). Саме нормалізація робить можливим порівняння «різнорідних» подій і побудову причинно-наслідкових ланцюгів між ними.У середній частині рисунка показано ядро кореляції – механізм у системі керування інформацією та подіями безпеки, який поєднує кореляцію за правилами (для чітко визначених індикаторів і порушень політик) та корелятор машинного навчання (для нетривіальних залежностей і слабких, розподілених у часі сигналів).

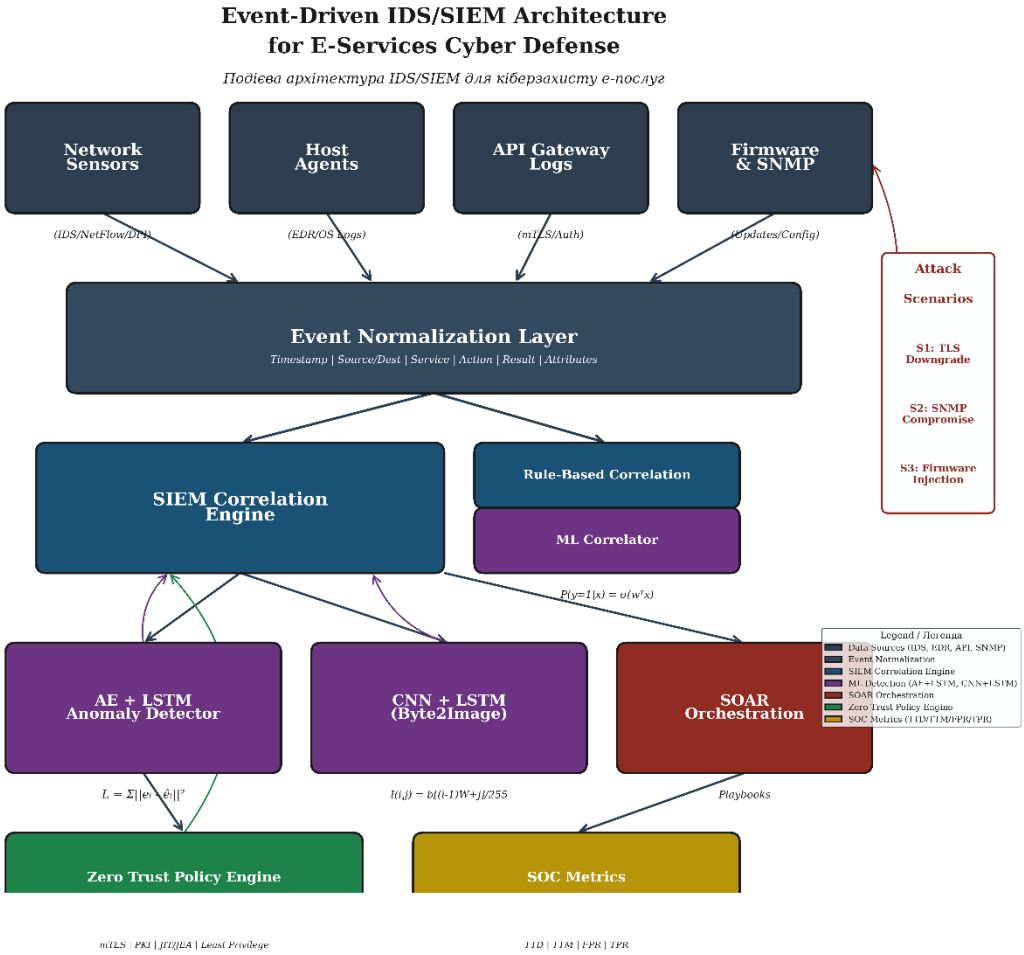

Рис. 1. Подієво-орієнтована архітектура кіберзахисту електронних послуг

Нижче відображено два нейромережеві детектори аномалій: (а) автокодер у поєднанні з рекурентною мережею довгої короткочасної пам'яті, який працює з послідовностями подій і використовує реконструкційну помилку як індикатор відхилення; (б) згорткова нейронна мережа у зв'язці з рекурентною мережею, яка аналізує «зображення» байтових вікон (перетворення байтів у зображення) для пошуку структурних відмінностей у бінарних або пакетних даних. Праворуч наведено приклади класів атак, для яких архітектура призначена: примусове зниження параметрів захищеного з'єднання, компрометація мережевого керування та ін'єкція модифікованої прошивки. У нижній частині відображено дві площини реакції та контролю: (1) рушій політик нульової довіри, який задає та примусово застосовує правила доступу (взаємна автентифікація сервісів, керування сертифікатами, мінімальні привілеї), і (2) оркестрація реагування з плейбуками, що зменшують час до пом'якшення наслідків. Завершує схему блок метрик центру операцій безпеки, який фіксує результативність (час до виявлення, час до пом'якшення наслідків, частки хибних спрацювань) і забезпечує зворотний зв'язок для налаштування правил та порогів моделей.

Подієвий контур IDS/SIEM та кореляція

Мережеві датчики IDS (аналіз потоків NetFlow/IPFIX та/або DPI) і хостові агенти (журнали ОС, аудит автентифікацій, EDR-телеметрія) формують події різної гранулярності [13]. Нормалізація виконується через узгоджену схему полів: час, джерело/призначення, сервіс, дія, результат, атрибути (TLS-версія, cipher suite, тип SNMP-операції, OID, код завершення), ідентифікатори активів та рольовий контекст. Далі події потрапляють у SIEM для:

- правил кореляції (ланцюги подій з часовими вікнами, підміткою контексту активів і зон сегментації);
- статистичних та ML-моделей, що оцінюють відхилення поведінки;
- оркестрації реагування (SOAR-плейбуки) для зменшення TTM [15].

Ймовірність інциденту $y = 1$ за набором ознак x (правила, контекст, ML-скори) оцінюється логістичною моделлю ризику:

$$P(y = 1|x) = \sigma(w^T x) = \frac{1}{1+\exp(-w^T x)}\ , \tag{2}$$

де w – ваги, що калібруються на історичних інцидентах, а x включає як детерміновані ознаки (спрацювання правила), так і неперервні (аномальний скор, критичність активу, репутаційні показники, оцінки вразливостей). Така модель є зручною для прозорої інтеграції rule-based і ML-компонентів у єдиному скорингу пріоритетів інцидентів [14].

AE+LSTM для послідовностей подій і трафіку

Нехай $\{e_t\}_{t=1}^T$ – послідовність нормалізованих подій у вікні T, поданих у вигляді векторів ознак $e_t \in \mathbb{R}^d$. Автокодер з LSTM-енкодером/декодером навчається мінімізувати реконструкційну помилку:

$$\mathcal{L}_{AE} = \sum_{t=1}^T \|e_t - \hat{e}_t\|_2^2\ , \tag{3}$$

де $\hat{e}_t$ – відновлення. Аномальність у вікні визначається як $\mathcal{A} = \frac{1}{T}\sum_{t=1}^T \| e_t - \hat{e}_t \|_2^2$, а поріг τ підбирається за заданим рівнем хибнопозитивних спрацювань у валідації. AE+LSTM добре відтворює «нормальні» патерни і підсвічує як підозрілу послідовність, так і її фрагменти, що особливо корисно для «повільних» атак зі слабким сигнатурним профілем [18, 16].

CNN+LSTM та Byte2Image для бінарних/пакетних структур

Для аналізу артефактів прошивок або «вікон» мережевих пакетів застосовується Byte2Image. Нехай бінарний фрагмент $b \in \{0, \dots, 255\}^N$ відображається у матрицю $I \in \mathbb{R}^{H\times W}$ так, що $HW = N$:

$$I_{i,j} = \frac{b_{(i-1)W+j}}{255}\ , \tag{4}$$

після чого CNN виділяє локальні патерни (наприклад, характерні структури заголовків, таблиці рядків SNMP, блоки сертифікатів), а LSTM моделює послідовність «зображень» у часі [19, 17]. Для навчання класифікатора використовується зважена крос-ентропія:

$$\mathcal{L}_{cls} = -\sum_{c\in\{0,1\}} \alpha_c\, y_c \log \hat{y}_c\ , \tag{5}$$

де α_c компенсує дисбаланс класів, y_c – істинні мітки (норма/атака), $\hat{y}_c$ – прогнози. Byte2Image застосовується «коли це доречно»: зокрема, для стабільних форматів (певні прошивки, пакети керування, структуровані дампи), а не для випадкового шифротексту, де просторові патерни неінформативні.

Оцінка TTD/TTM та інтегрований критерій ефективності

Для SOC важливими є час до виявлення (TTD) та час до пом'якшення наслідків (TTM) [21]. Для порівняння архітектур вводиться нормований інтегрований критерій:

$$J = \lambda_1 \frac{\text{TTD}}{\text{TTD}_0} + \lambda_2 \frac{\text{TTM}}{\text{TTM}_0} + \lambda_3 \text{FPR} + \lambda_4 (1 - \text{TPR})\ , \tag{6}$$

де TTD_0, TTM_0 – базові значення (наприклад, IDS-only), FPR – частка хибнопозитивних, TPR – частка істиннопозитивних (recall), λ_i – ваги, узгоджені з пріоритетами організації та критичністю послуг.

Наведені в розділі методи формують цілісну, відтворювану схему перевірки цільової архітектури кіберзахисту електронних послуг: від проєктування контуру нульової довіри (сегментація доменів, політики доступу, взаємна автентифікація сервісів і керування сертифікатами) до побудови подієвого контуру моніторингу (мережеві та хостові джерела подій, нормалізація полів, кореляція у системі керування інформацією та подіями безпеки) і керованого реагування через плейбуки оркестрації. Ключовим методичним рішенням є дворівнева кореляція: правила фіксують порушення політик і явні індикатори, а статистично-аналітичний шар доповнює їх оцінкою ризику та пошуком прихованих залежностей у часі й між сенсорами.

Модулі виявлення аномалій інтегровані як «підсилювач» кореляції, а не як її заміна: автокодер із рекурентною мережею застосовано для послідовностей подій і трафіку з порогуванням за реконструкційною помилкою, а для структурованих бінарних або пакетних даних використано перетворення байтових послідовностей у зображення та згортково-рекурентну модель. Така постановка забезпечує поєднання інтерпретованості (через правила і явні атрибути подій) та стійкості до «повільних» багатокрокових сценаріїв (через поведінкові відхилення), що критично для атак на захищені з'єднання, мережеве керування і ланцюги оновлення вбудованого програмного забезпечення. Отже, методи визначають і порядок експерименту, і критерії оцінювання: порівняння архітектурних варіантів виконується за операційними показниками центру операцій безпеки (час до виявлення, час до пом'якшення наслідків, частки хибних спрацювань, покриття сценаріїв) та якістю моделей (узагальнювальні метрики класифікації й ранжування). У наступному розділі «Результати» наведено сценарії моделювання гібридних атак, спостережувані прояви у телеметрії та порівняльні таблиці, які демонструють, як запропонована конфігурація впливає на швидкість і точність детекції та на зниження шуму інцидентів.

Результат

У цьому розділі наведено результати експериментальної перевірки запропонованої цільової архітектури кіберзахисту електронних послуг, що поєднує контур нульової довіри, подієвий контур моніторингу та кореляції і модулі виявлення аномалій на основі глибокого навчання. Оцінювання виконано за сценарійним принципом на відтворюваних гібридних атаках, де одночасно задіюються мережеві взаємодії, керування та ланцюг оновлення вбудованого програмного забезпечення.

Такий підхід дозволяє перевірити не «абстрактну» точність детектора, а практичну спроможність архітектури скорочувати час до виявлення та час до пом'якшення наслідків, зменшуючи шум інцидентів при збереженні покриття сценаріїв [6, 12, 15].Далі результати структуровано у трьох площинах.

По-перше, описано змодельовані сценарії та їх спостережувані прояви в телеметрії, з фокусом на атаках на захищений транспортний рівень і керувальні протоколи та на прошивкових векторах, що узгоджується з вимогами архітектури нульової довіри і практиками кореляції багатошарових атак [6, 14, 15].

По-друге, наведено порівняльні метрики на рівні центру операцій безпеки для трьох архітектурних варіантів (лише датчики, датчики з кореляцією, повний варіант із нульовою довірою та машинним навчанням), що демонструє вплив поєднання сегментації, нормалізації та кореляції на операційну ефективність реагування [7, 15, 21].

По-третє, подано якість нейромережевих компонентів для часових послідовностей та структурованих даних, включно з обґрунтуванням вибору метрик для дисбалансних класів і прикладом оперативних розрахунків, що забезпечує відтворюваність і придатність результатів до практики впровадження у середовищах електронних послуг [4, 5, 13, 16, 20].

Сценарії моделювання гібридних атак та спостережувані прояви

Синтетичні сценарії формуються так, щоб їх можна було відтворити в лабораторії або в пісочниці DevSecOps без витоку чутливих даних. Під «гібридністю» мається на увазі комбінування щонайменше двох площин: (i) мережевої взаємодії, (ii) керування/адміністрування, (iii) firmware-ланцюга. Події знімаються з мережевого сенсора (потоки + метадані TLS), хостових журналів автентифікації та системних повідомлень, журналів оновлення, а також із SNMP-телеметрії.

Сценарій S1 (TLS downgrade / помилкова валідація). Ознаки: невідповідність очікуваної версії TLS політикам сервісу, нетиповий вибір cipher suite, повторні handshake-спроби, а також розходження між SNI/сертифікатом і дозволеним профілем сервісу [6, 5, 23]. SIEM-правила фіксують downgrade/помилки валідації, а AE+LSTM підтверджує аномальність за контекстом сесії (нетипова послідовність подій «збої handshake → повторні спроби → успішний доступ при нижчій версії», а також супровідні хостові події).

Сценарій S2 (компрометація SNMP). Ознаки: запити з неавторизованих сегментів, часті get-bulk на критичних OID, поява set-request (write-access), зміни конфігурацій інтерфейсів, перезапуски сервісів [7, 29, 8]. Для середовищ, де ще використовується SNMPv2c, сигналом ризику є спроба доступу з нехарактерного джерела навіть без явного set-request, оскільки зловмисник може «розігрівати» розвідку перед змінами.

Сценарій S3 (firmware через ланцюг оновлення). Ознаки: аномальні запити до серверів оновлень, відхилення хешів/підписів, «стрибки» версій, поява нових мережевих залежностей після оновлення, зміни у TLS-поведінці бібліотек, приховані SNMP-команди [11, 9, 10, 24]. Для артефактів прошивок застосовується Byte2Image + CNN+LSTM, що виявляє структурні відхилення у сегментах бінарника (наприклад, нетипові таблиці рядків, додаткові секції, повторювані шаблони інструкцій).

Порівняльна оцінка архітектурних варіантів

Розглянуто три варіанти: A) IDS-only (базовий), B) IDS+SIEM (rule-based), C) Zero Trust + IDS+SIEM + ML (запропонований). Табл. 1 демонструє узагальнені метрики SOC-рівня, отримані на однаковому наборі сценаріїв (S1–S3) із повтореннями та варіаціями інтенсивності.

Таблиця 1

Порівняння варіантів архітектури за метриками SOC

Варіант	TTD, хв	TTM, хв	FPR	Покриття сценаріїв
A: IDS-only	18.4	62.0	0.14	S1 частково, S2 частково
B: IDS+SIEM (rules)	7.9	28.5	0.11	S1, S2, S3 частково
C: ZT+IDS+SIEM+ML	3.1	12.7	0.06	S1--S3 повне

Скорочення TTD у варіанті C забезпечується: (i) сегментацією і явними політиками (менше «сірих зон»), (ii) контекстною кореляцією в SIEM, (iii) ML-детекцією аномальних послідовностей та бінарних артефактів. Зниження FPR пояснюється тим, що ML-модулі застосовуються як підсилювач кореляції: аномальний скор піднімає пріоритет лише при виконанні контекстних умов (критичний актив, порушення політики, пов’язаний індикатор). Відповідно, аналітик SOC отримує менший обсяг шумових алертів і швидше переходить до реакції.

Якість моделей AE+LSTM та CNN+LSTM

Таблиця 2 узагальнює метрики моделей на тестових вибірках, сформованих за сценаріями. Для дисбалансних класів застосовано зважування втрат (5) і калібрування порогу аномальності (3). Для інтерпретації PR-AUC використано рекомендацію про доцільність precision-recall аналізу при рідкісних подіях [20].

© Яковенко В.О., Мормуль М.Ф. Проєктування кіберзахисту електронних сервісів у процесі реінжинірингу: нульова довіра, подієва аналітика та детекція прошивкових і мережевих атак методами глибокого навчання. Сучасний захист інформації, 1(65), 149–163.
https://doi.org/10.31673/2409-7292.2026.011827

Таблиця 2

Порівняння моделей детекції аномалій за метриками якості

Модель	F1	ROC-AUC	PR-AUC	Примітка
AE+LSTM (події/потоки)	0.89	0.94	0.91	краща для ``повільних'' атак
CNN+LSTM (Byte2Image)	0.86	0.92	0.88	чутлива до firmware/структур
Rule-only (baseline)	0.74	0.81	0.76	залежить від покриття правил

Практичний висновок: AE+LSTM доцільно ставити на траєкторії «події → сесії → інциденти», тоді як CNN+LSTM доцільно використовувати точково – для артефактів прошивок, дампів оновлень або для коротких пакетних «байтових вікон», де структури відносно стабільні [19, 17]. Byte2Image працює найкраще, коли формат даних має повторювані патерни, а не при домінуванні випадкового шифротексту.

Приклад MATLAB Mobile коду для оперативного розрахунку TTD/TTM

Нижче наведено приклад для швидкого оцінювання TTD/TTM за журналами часових міток у MATLAB Mobile. Код може бути адаптований під формати CSV/JSON, що вивантажуються з SIEM або SOAR.

Розвиток електронних послуг у державному та корпоративному секторі зумовив потребу у вбудованому кіберзахисті, який охоплює не лише мережеві компоненти, а й firmware-ланцюги, протоколи керування та інфраструктуру оновлень. Класичні моделі периметрового захисту більше не гарантують безпеки в умовах мікросервісних і гібридних середовищ. У таких системах компрометація одного вузла може призводити до каскадних наслідків, тому необхідно забезпечити цілісну архітектуру виявлення та реагування, що спирається на принцип нульової довіри (Zero Trust), подієву кореляцію IDS/SIEM і машинне навчання для поведінкової детекції.Підхід Zero Trust формалізує ідею, що жоден суб’єкт або пристрій не є довіреним за замовчуванням, а всі запити проходять перевірку контексту, політик і стану середовища. У поєднанні з подієвим контуром моніторингу це дозволяє зменшити площу атаки, швидше виявляти інциденти й автоматизувати реакцію. Водночас гібридні атаки, які включають firmware-модифікації, зниження рівня TLS або маніпуляції SNMP, потребують аналітичних модулів глибокого навчання, здатних розпізнавати нетипові часові послідовності та структурні відхилення у даних.З огляду на це, побудовано експериментальну архітектуру кіберзахисту е-послуг, де інтегруються три рівні: Zero Trust-контур, IDS/SIEM-кореляція та ML-детекція аномалій. Для її оцінювання застосовано комплексну візуалізацію SOC-метрик, яка узагальнює операційні показники часу реагування, точності та повноти покриття сценаріїв.

Рисунок 2. Опис комплексної візуалізації

(a) TTD та TTM для архітектур A–C. Стовпчикова діаграма показує операційну швидкість SOC: час до виявлення (TTD) і час до пом’якшення наслідків (TTM). Видно перехід від повільнішого A до швидшого C: A = 18.4/62.0 хв, B = 7.9/28.5 хв, C = 3.1/12.7 хв (TTD/TTM).

(b) FPR і покриття сценаріїв S1–S3. Тут фіксується «ціна шуму» (частка хибнопозитивних) і те, наскільки архітектура реально закриває сценарії атак. У даних порівняння FPR зменшується від A до C (0.14 → 0.11 → 0.06), а покриття переходить від часткового до повного для S1–S3 у варіанті C.

(c) Інтегрований критерій J (формула 6). Це «зведений індикатор» для швидкого ранжування архітектур, який агрегує ключові метрики (з вагами під пріоритети організації). Його сенс у візуалізації - дати один зрозумілий підсумок там, де окремі метрики можуть “тягнути” в різні боки. Формально критерій вводиться як нормований показник для порівняння архітектур.

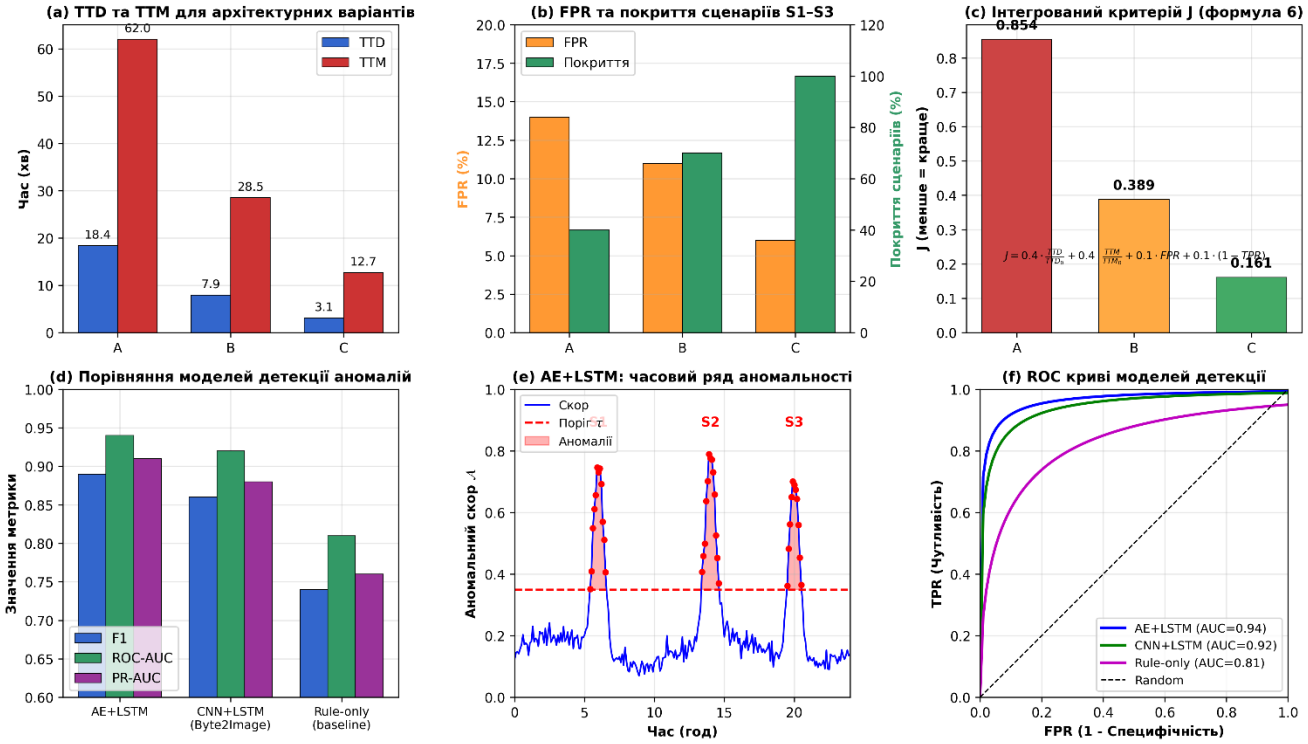

Рис. 2. Комплексна візуалізація SOC-метрик для архітектури кіберзахисту е-послуг Zero Trust + IDS/SIEM + ML детекція аномалій

(d) Порівняння моделей детекції аномалій. Діаграма узагальнює F1, ROC-AUC та PR-AUC для AE+LSTM, CNN+LSTM (Byte2Image) і rule-only baseline. За наведеними результатами найкращу якість дає AE+LSTM (F1=0.89, ROC-AUC=0.94, PR-AUC=0.91), далі CNN+LSTM (0.86/0.92/0.88), а rule-only поступається (0.74/0.81/0.76).

(e) Приклад AE+LSTM у часі (аномальний скор). Графік часового ряду демонструє, як реконструкційна помилка (або аномальний скор) формує «піки» на епізодах атак; пунктирний поріг відокремлює норму від аномалій. Ідея проста: правило може “побачити” окрему ознаку, а AE+LSTM підсвічує нетипову послідовність подій як цілісний патерн (особливо корисно для “повільних” атак).

(f) ROC-криві моделей. Криві наочно порівнюють здатність моделей відділяти норму від атак за різних порогів; площі під кривою (AUC) узгоджуються з табличними значеннями (AE+LSTM вище за CNN+LSTM, а rule-only суттєво нижче).

Ключовий висновок, який підсумовує вся композиція: у варіанті C скорочується TTD, зменшується FPR і підвищується покриття, оскільки ML використано як підсилювач кореляції (аномальний скор піднімає пріоритет лише за контекстних умов), а не як «самодостатню магію».

Нижче подано оновлені фрагменти 4 Discussion / Обмеження / Перспективи так, щоб усі посилання були лише в межах [1-17] і узгоджувалися з логікою Вашого тексту (в т.ч. заміна [18, 19, 24–27 тощо], які зараз присутні у файлі).

Дискусія

Порівняно з підходами, орієнтованими лише на мережеві сигнатури IDS або ізольовані журнали, запропонована архітектура системно інтегрує три шари: архітектурний (Zero Trust), подієвий (IDS → нормалізація → SIEM) та аналітичний (ML для аномалій). Це відповідає сучасному зсуву від «точкових» контролів до кібербезпеки як системної властивості підприємства, де безпека визначається взаємодією сервісів, процесів та активів [1]. Нульова довіра формалізує безперервну перевірку й контекстну авторизацію [6], а патерни

проєктування Zero Trust для розподілених/кіберфізичних середовищ підкреслюють необхідність мікросегментації та керованих рішень доступу [14]. На практиці, ефект проявляється не декларативно, а через вимірювані SOC-показники (TTD/TTM) та зниження операційного «шуму», що узгоджується з роллю кореляційних механізмів SIEM для багатошарових атак [15] і базовими настановами побудови IDPS [12].Важлива відмінність від «ML-first» підходів полягає у ролі нейромереж: вони не замінюють правила, а доповнюють їх у дворівневій кореляції. Детерміновані правила фіксують порушення політик (наприклад, невідповідні параметри захищеної сесії або керувальні операції з недозволених сегментів), тоді як поведінкові моделі виявляють нетипові послідовності та слабкі розподілені у часі сигнали. Для часових рядів подій релевантними є LSTM-орієнтовані підходи та енкодер-декодер для мультисенсорних аномалій [4, 5], для мережевих потоків – гібридні C-LSTM моделі [13], а для середовищ SDN/IoT - CNN-LSTM детектори, що поєднують «просторові» та часові залежності [16, 17]. Для структурованих бінарних/пакетних фрагментів доцільне Byte2Image-подання, яке має підтверджену придатність для класифікації модифікованих бінарних об’єктів [3]. У сукупності це підвищує інтерпретованість кореляції: правила задають причинні «якорі», а ML додає раннє підсвічування нетипових траєкторій, що зменшує FPR без втрати покриття сценаріїв.Порівняння з логікою Zero Trust показує, що сегментація і контекстний доступ зменшують площу атаки, однак не гарантують виявлення інцидентів без кореляції та збагачення подій контекстом активів і процесів [6, 14]. Це особливо критично для вбудованих мережевих пристроїв, де керувальна площина і прошивкові зміни можуть маскуватися під легітимні адміністративні дії, що підтверджено широкомасштабними спостереженнями щодо небезпечності цього класу активів [10]. Отже, практичний мінімум для е-послуг доцільно формалізувати як: (i) mTLS/PKI та надійна валідація сертифікатів у межах моделі нульової довіри [6]; (ii) ізоляція керувальних мереж і контроль керувальних операцій у сегментованій архітектурі [14]; (iii) контроль і аудит вбудованих пристроїв і пов’язаних із ними змін конфігурацій/оновлень як окремої площини ризику [10]; (iv) вимірюваний подієвий контур IDS/SIEM з кореляцією багатошарових сценаріїв [12, 15].

Обмеження

По-перше, якість ML-детекції залежить від репрезентативності датасетів і стабільності «норми» у часі. У реальних SOC спостерігається дрейф через оновлення сервісів, зміну політик доступу та еволюцію трафіку; тому потрібні процедури керованого перегляду базових ліній, калібрування порогів і контроль якості даних у циклі безперервного вдосконалення, що узгоджується з настановами щодо вимірюваності та управління ризиком [7]. Додатково, для контролю змін у «траєкторіях» інцидентів доцільно застосовувати процесний аналіз подій (process mining) як інструмент виявлення нетипових варіацій процесів реагування й появи нових шляхів компрометації [11], у поєднанні з кореляційними механізмами SIEM [15].По-друге, Byte2Image-представлення є ефективним лише там, де дані мають достатньо стабільні структурні патерни; у протилежному випадку (наприклад, при домінуванні випадковоподібного шифротексту) воно може втрачати семантику протоколу/структури. Це вимагає або доменної сегментації вхідних «вікон» за кордонами структур, або комбінування з більш придатними для мережевого трафіку часовими моделями [13]. Практично, Byte2Image доцільно застосовувати точково для артефактів, подібних до тих, що розглядаються у роботах з візуалізації/класифікації бінарних об’єктів [3], а для мереж SDN/IoT - підсилювати CNN-LSTM підходами, орієнтованими на змішані просторово-часові залежності [16, 17].По-третє, правила SIEM можуть бути обійдені «повільними» атаками з низькою інтенсивністю або з розподілом дій у часі. У таких випадках зростає роль поведінкового моделювання та збільшених часових вікон кореляції, однак це потребує зрілої інженерії даних, якісної нормалізації подій і дисципліни процесів SOC, що відповідає профільним рекомендаціям щодо IDPS та практикам кореляції багатошарових атак [12, 15]. Для таких сценаріїв найбільш

релевантними є LSTM-підходи до аномалій у часових рядах і мультисенсорні енкодер-декодер архітектури [4, 5].

Перспективи: Zero Trust і multimodal AI

Наступним кроком розвитку є перехід до повноцінної багатоджерельної (мультимодальної) аналітики, де поєднуються журнали, мережеві часові ряди, артефакти вбудованих компонентів і контекст активів/процесів у єдиному механізмі кореляції. Практично це доцільно інтерпретувати як «інцидентний граф», де вузли відповідають подіям і активам, а ребра - причинно-наслідковим залежностям, політикам та типовим траєкторіям процесів. Такий підхід добре узгоджується з ідеєю цифрових двійників виробничих/сервісних систем як контекстного шару для спостереження й порівняння станів [8, 9] та з кореляційною логікою SIEM для багатошарових атак [15]. Для «пояснюваності» рішень і покращення плейбуків реагування перспективним є поєднання SIEM-кореляції з процесним майнінгом, який відновлює типові сценарії інцидентів і дає прозорі «маршрути» відхилень [11].Для Zero Trust перспективними залишаються fine-grained авторизація та контекстні політики доступу з опорою на безперервну перевірку, ротацію довіри та формалізовані патерни проєктування для розподілених середовищ [6, 14]. З огляду на те, що вибір архітектурних параметрів і налаштувань аналітики неминуче є компромісом між швидкістю реагування, точністю, ресурсами SOC і вартістю впровадження, доцільно формалізувати подальшу оптимізацію як багатокритеріальну задачу з явними вагами цілей [2] у межах вимірюваного циклу кібербезпеки [7]. Окремий практичний напрям - розширення поведінкової детекції для SDN/IoT і вбудованих мережевих пристроїв, де релевантними є CNN-LSTM підходи для аномалій у шумних багатоджерельних середовищах [16, 17] та врахування специфічних ризиків вбудованих активів як окремої площини атаки [10].

Висновки

У роботі сформовано цілісну TO-BE архітектуру кіберзахисту е-послуг у контексті реінжинірингу, де безпека розглядається не як набір розрізнених засобів, а як узгоджений контур керування доступом, подій та аналітики. Інтеграція Zero Trust із мікросегментацією, mTLS/PKI, мінімальними привілеями та політиками адміністрування створює керований «скелет» довіри й доступу, який зменшує площу атаки та дисциплінує взаємодію сервісів, але водночас вимагає якісного подієвого шару, щоб ця дисципліна була спостережуваною і перевірюваною в експлуатації. Саме тому подієвий контур IDS/SIEM із нормалізацією і кореляцією виступає центральним механізмом операційної керованості: він перетворює розрізнені сигнали від мережі, хостів і сервісів на інцидентні гіпотези, придатні для реагування та аудиту.Експериментальна перевірка на синтетичних сценаріях, що охоплюють деградацію SSL/TLS, помилки валідації, компрометацію керувальної площини через SNMP та firmware-атаки в ланцюгах оновлення, підтвердила практичну перевагу інтегрованого підходу над ізольованими IDS або виключно rule-based кореляцією.

Досягнуто скорочення часу до виявлення та часу до пом’якшення наслідків, зменшення частки хибнопозитивних спрацювань і водночас зростання покриття сценаріїв, тобто система стала одночасно швидшою, «тихішою» для операторів і більш повною за змістом. Це принципово важливо для SOC, бо саме поєднання швидкості з низьким шумом визначає, чи зможе команда реагувати на інциденти в реальному темпі, а не в режимі постійного «розгрібання» алертів.Показано, що найбільш життєздатною є гібридна модель, де правила не витісняються нейромережами, а задають політичний і причинний каркас контролю, тоді як ML-компоненти підсилюють кореляцію, виявляють нетипові послідовності та приховані залежності, які часто не мають однозначної сигнатури. Такий розподіл ролей підвищує інтерпретованість рішень: правила відповідають на питання «що саме порушено», а моделі аномалій дають відповідь «що виглядає нетипово і чому це варто підняти в пріоритет». Практично це означає, що SOC отримує не лише більше сигналів, а сигналів більшої якості, які краще пояснюються і швидше перетворюються на дії.

Окремим висновком є необхідність виділяти керувальну площину та firmware-ланцюг як повноцінні об’єкти контролю на рівні архітектури, а не як «додаток» до класичних мережевих політик. Навіть за правильно налаштованих TLS-політик і сегментації існують обхідні траєкторії через адміністративні протоколи, конфігурації та оновлення, які можуть легітимізувати шкідливі зміни. Тому практичний мінімум впровадження має включати контроль доступу й секретів у керувальних сегментах, обмеження операцій запису, аудит і журналювання адміністративних дій, а також керовані механізми оновлень із перевіркою цілісності, атестацією та контролем постачальницьких залежностей.

Підкреслено, що оцінювання ефективності подібних архітектур не може зводитися лише до метрик якості моделей на кшталт F1 або ROC-AUC. Для інженерного вибору та експлуатаційного управління ключовими залишаються SOC-метрики, які прямо відображають цінність для реагування, а також інтегрований критерій, що дозволяє агрегувати компроміси між швидкістю, точністю, шумом і покриттям у зрозумілий показник для прийняття рішень. У підсумку запропонований підхід забезпечує керовану, вимірювану й практично придатну рамку кіберзахисту е-послуг, де архітектурні рішення, моніторинг і аналітика працюють як одна система, а не як набір інструментів, що випадково опинилися поруч.

Перелік посилань

1. von Solms R., van Niekerk J. From information security to cybersecurity // Computers & Security. 2013. Vol. 38. P. 97–102. DOI: https://doi.org/10.1016/j.cose.2013.04.004.

2. Marler R. T., Arora J. S. Survey of multi-objective optimization methods // Structural and Multidisciplinary Optimization. 2004. Vol. 26. P. 369–395. DOI: https://doi.org/10.1007/s00158-003-0368-6.

3. Nataraj L., Karthikeyan S., Jacob G., Manjunath B. S. Malware images: visualization and automatic classification // Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec 2011). 2011. P. 1–7. DOI: https://doi.org/10.1145/2016904.2016908.

4. Nguyen V. Q., Ma L., Kim J. LSTM-based anomaly detection on big data for smart factory monitoring // Journal of Digital Contents Society. 2018. Vol. 19, No. 4. P. 789–799. DOI: https://doi.org/10.9728/dcs.2018.19.4.789.

5. Malhotra P., Ramakrishnan A., Anand G., Vig L., Agarwal P., Shroff G. LSTM-based encoder–decoder for multi-sensor anomaly detection // Proceedings of the ICML 2016 Workshop on Anomaly Detection. 2016. DOI: https://doi.org/10.48550/arXiv.1607.00148.

6. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture : NIST Special Publication 800-207. Gaithersburg : NIST, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207.

7. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0 : NIST CSWP 29. Gaithersburg : NIST, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

8. Tao F., Qi Q., Wang L., Nee A. Y. Digital twins and cyber-physical systems toward smart manufacturing and industry 4.0: correlation and comparison // Engineering. 2019. Vol. 5. P. 653–661. DOI: https://doi.org/10.1016/j.eng.2019.01.014.

9. Kritzinger W., Karner M., Traar G., Henjes J., Sihn W. Digital Twin in manufacturing: a categorical literature review and classification // IFAC-PapersOnLine. 2018. Vol. 51, No. 11. P. 1016–1022. DOI: https://doi.org/10.1016/j.ifacol.2018.08.474.

10. Cui A., Stolfo S. A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan // Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC 2010). 2010. P. 97–106. DOI: https://doi.org/10.1145/1920261.1920276.

11. van der Aalst W. M. P. Process Mining: Data Science in Action. 2nd ed. Berlin ; Heidelberg : Springer, 2016. 467 p. DOI: https://doi.org/10.1007/978-3-662-49851-4.

12. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS) : NIST Special Publication 800-94. Gaithersburg : NIST, 2007. DOI: https://doi.org/10.6028/NIST.SP.800-94.

13. Kim T. Y., Cho S. B. Web traffic anomaly detection using C-LSTM neural networks // Expert Systems with Applications. 2018. Vol. 106. P. 66–76. DOI: https://doi.org/10.1016/j.eswa.2018.04.004.

14. Hasan S., Raza M., Ghosh S., et al. Zero-trust design and assurance patterns for cyber–physical systems // Journal of Systems Architecture. 2024. DOI: https://doi.org/10.1016/j.sysarc.2024.103261.

15. Sheeraz M., Durad M. H., Paracha M. A., Mohsin S. M., Kazmi S. N., Maple C. Revolutionizing SIEM Security: An Innovative Correlation Engine Design for Multi-Layered Attack Detection // Sensors. 2024. Vol. 24, No. 15. Art. 4901. DOI: https://doi.org/10.3390/s24154901.

16. Abdallah M., Le-Khac N.-A., Jahromi H. Z., Jurcut A. D. A Hybrid CNN-LSTM Based Approach for Anomaly Detection Systems in SDNs // Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021). 2021. DOI: https://doi.org/10.1145/3465481.3469190.

17. Hussain O. A., Chen Z., et al. sSecure Net: A Hybrid CNN-LSTM-based Intrusion Detection System for Securing IoT Networks // Proceedings (ACM). 2025. DOI: https://doi.org/10.1145/3727648.3727736.

Надійшла до редакції (Received): 24.02.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

УДК 621.396.93:623.746-519
DOI: 10.31673/2409-7292.2026.011239

Синявський О. Ю.

МЕТОД РОЗРАХУНКУ ЧУТЛИВОСТІ КАНАЛУ ЗВ'ЯЗКУ БПЛА ЯК КРИТЕРІЮ СИНТЕЗУ СИГНАЛІВ УПРАВЛІННЯ

Помилки при управлінні безпілотними літальними апаратами (БПЛА) є причинами їх втрати та не виконання завдань функціонального призначення за рахунок збільшення траєкторії польоту, що не передбачено польотним завданням. Оптимальне значення чутливості каналу зв'язку БПЛА дозволяє підвищити надійність управління при незначних енергетичних складових сигналу. Такий висновок обумовлено тим, що необхідно визначити оптимальне відношення сигнал / завада каналу зв'язку БПЛА відносно необхідної дальності управління та захищеності операторів. Критерії оптимізації характеристик сигналу управління каналів зв'язку БП-ЛА. Метою статті є розробка методу розрахунку чутливості каналу зв'язку БПЛА як критерію синтезу сигна-лів управління для забезпечення надійного управління. Розроблено метод розрахунку чутливості каналу зв'язку БПЛА для забезпечення надійного управління. Розроблений метод пропонується застосовувати при обґрунтуванні характеристик сигналів управління каналу зв'язку БПЛА для забезпечення раціонального поєднання відношення сигнал / завада на вході приймача каналу зв'язку, надійного управління при польоту та незначної витрати коштів на об'єкти разової дії. Розроблений критерій чутливості каналу зв'язку БПЛА для забезпечення надійного управління характеризує час розповсюдження сигналу каналом зв'язку БПЛА та впливає на надійність управління в умовах протидії противника. Подальші дослідження пропонується направити на обґрунтування інших критеріїв оптимальності синтезу характеристик сигналу управління каналу зв'язку БП-ЛА та проведення їх порівняння.

Ключові слова: БПЛА, засіб, захищеність, інформація, канал зв'язку, математична модель, синтез, спостереження, радіоелектронна протидія, радіотехнічні завади, управління, чутливість.

Вступ

Помилки при управлінні безпілотними літальними апаратами (БПЛА) можуть привести до їх втрати та не виконання завдань функціонального призначення за рахунок збільшення траєкторії польоту, що не передбачено польотним завданням [1-4]. Для забезпечення надійності управління БПЛА при польоті використовують радіосигнали відносно значної потужності для забезпечення дальності дії каналу зв'язку та боротьби із засобами протидії противника. Однак, значна потужність сигналу управління БПЛА для забезпечення надійності функціонування каналу зв'язку є демаскуючим фактором для операторів, що підтверджено результатами ведення антидронової боротьби у сучасних військових конфліктах, у тому числі на території України [4-8].

Постановка проблеми

На сьогодні для розв'язання питання захисту від завад радіосигналів управління каналів зв'язку БПЛА та прихованості дії операторів широко використовується оптоволоконна лінія [3, 9]. Однак застосування оптоволоконної лінії управління збільшує не тільки вартість БПЛА, але й накладання особливостей їх застосування в умовах активної протидії: використання лазерних ножів, періодичне механічне перерізання ліній наземними роботизованими комплексами, встановлення термальних ліній в секторі дії дронів тощо. Тому актуальним досі