DOI: 10.18372/2310-5461.69.20945
УДК 004.056.53 (045)

***А. В. Ільєнко*,** канд. техн. наук, доцент
Державний університет «Київський авіаційний інститут»
https://orcid.org/0000-0001-8565-1117
e–mail: anna.ilienko@ npp.kai.edu.ua;

***С. С. Ільєнко*,** канд. техн. наук, доцент
Державний університет «Київський авіаційний інститут
https://orcid.org/0000-0002-0437-0995
e–mail: serhii.ilienko@npp.kai.edu.ua;

***В. А. Телющенко*,** аспірант
Державний університет «Київський авіаційний інститут
https://orcid.org/0000-0001-6026-5105
e–mail: valentyna.teliushchenko@npp.kai.edu.ua;

С.Д. Маляренко
Державний університет «Київський авіаційний інститут
https://orcid.org/0009-0003-2843-6076
e–mail: maliarenko.sofiia@gmail.com

ТЕОРЕТИЧНИЙ ПІДХІД ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ОЦІНКИ РИЗИКІВ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вступ

Сучасне функціонування об'єктів критичної інфраструктури (КІ) визначається високим рівнем взаємопроникнення інформаційних та операційних технологій, унаслідок чого кіберзагрози безпосередньо впливають на стабільність надання суспільно значущих послуг. Активне впровадження хмарних платформ, механізмів дистанційного керування, промислових IoT-рішень і сервісних моделей із залученням сторонніх провайдерів істотно ускладнює архітектуру взаємодії систем та розширює поверхню потенційних атак на суб'єкти інформаційної діяльності. Водночас наявність структурних недоліків у промислових комунікаційних протоколах, а також обмежена гнучкість процесів оновлення в технологічних доменах спричиняють довготривалий період експлуатаційного ризику. Компрометація безпеки на рівні периферійних компонентів або в межах ланцюгів постачання може швидко набути системного характеру та призвести до масштабних міжгалузевих збоїв об'єктів критичної інфраструктури. За таких обставин традиційні, переважно реактивні, моделі управління ризиками не забезпечують належного рівня ефективності та потребують доповнення інтелектуалізованими інструментами, автоматизованими аналітичними методами й обґрунтованою пріоритизацією заходів із забезпечення захисту інформації та інформаційно-технологічного середовища в цілому.

Постановка завдання дослідження

У межах статті як об'єкт критичної інфраструктури розглянуто авіаційну галузь, а насамперед інформаційно-комунікаційні системи (ІКС) цивільної авіації (ЦА) (мережі та сервіси аеропортів і авіакомпаній, системи підтримки польотних операцій, сервіси управління пасажиропотоками та суміжна інженерна інфраструктура). Висока інтегрованість та взаємозалежність інформаційних технологій (ІТ) та операційних технологій (ОТ) у таких ІКС зумовлює підвищені вимоги до безперервності, сегментації та ризик-орієнтованого управління безпекою. У контексті цивільної авіації до ІТ відносять корпоративні мережі та прикладні сервіси (планування та супровід рейсів, обслуговування пасажирів, управління персоналом і ресурсами), тоді як ОТ охоплює технологічні сегменти та системи керування інженерною інфраструктурою аеропорту (зокрема SCADA/PLC для електропостачання, освітлення, кліматичних систем, багажних та інших технологічних ліній).

Інтегроване застосування міжнародних стандартів і галузевих настанов дозволяє вибудувати наскрізну методологію управління ризиками. Зокрема, Міжнародний стандарт ISO/IEC 27005 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки» визначає рамкові принципи функціонування процесу управління ризиками в складі системи управління інформаційними технологіями, включно з форма-

лізацією критеріїв прийнятності, розподілом ролей і механізмами взаємодії між зацікавленими сторонами. Документ NIST SP 800-30 «Guide for Conducting Risk Assessments», керівництво (посібник) з проведення оцінки ризиків інформаційних систем доповнює цю рамку деталізованим підходом до оцінювання ризиків, висуваючи вимоги до обґрунтованості припущень, шкалювання, використаних джерел даних і забезпечення простежуваності прийнятих рішень. Матеріали Агентство Європейського Союзу з кібербезпеки (European Union Agency for Cybersecurity, ENISA), у свою чергу, забезпечують актуальний загрозоорієнтований контекст та пов'язують положення Директиви про мережеву та інформаційну безпеку NIS2 (Network and Information Security Directive 2) з набором практично перевірюваних заходів безпеки. В умовах конвергенції IT/OT зазначений підхід конкретизується вимогами міжнародних стандартів IEC 62443, присвячених кібербезпеці систем промислової автоматизації та керування (Industrial Automation and Control Systems, IACS) щодо зонування, каналів взаємодії та цільових рівнів безпеки, що створює передумови для технічно здійсненної та аудитоздатної реалізації захисних механізмів. Сукупно це формує узгоджену й відтворювану методичну основу для системного зниження рівня ризику в об'єктах критичної інфраструктури.

Метою статті є наукове обґрунтування підходу до інтелектуалізованого оцінювання ризиків ІКС ЦА на основі методів машинного навчання, орієнтованого на підвищення своєчасності виявлення кіберзагроз і ефективності реагування з урахуванням вимог директив NIS2, Директива про стійкість критичних об'єктів CER (Critical Entities Resilience Directive,) та галузевих рекомендацій. Актуальність дослідження підтверджується оцінками ENISA Threat Landscape 2025, за якими авіаційний сегмент є одним із найбільш уражених у транспортній сфері, а типовий профіль інцидентів визначається атаками, що виводять цифрові сервіси з ладу (передусім DDoS), а також інцидентами кіберзлочинності, пов'язаними з програмами-вимагачами та витоками даних. Досягнення поставленої мети передбачає комплексний аналіз актуальних кіберзагроз і тенденцій їх еволюції, формування моделі машинного навчання як базового елемента системи із можливістю подальшого розширення за рахунок кластеризаційних, аномалієорієнтованих і регресійних методів, а також проєктування архітектури багаторівневої системи оцінки ризиків з інтеграцією методів машинного навчання, що забезпечує повний цикл обробки даних — від збору та формування ознак до інтеграції результатів оцінювання з SOC-центром суб'єктів критичної інфраструктури.

Аналіз останніх досліджень та публікацій

Загрози та уразливості критичної інфраструктури у сфері кібербезпеки

Кібербезпекові ризики КІ формуються внаслідок тісної взаємодії інформаційних і операційних технологій, де порушення властивостей конфіденційності, цілісності або доступності цифрових компонентів може спричиняти безпосередні фізичні та соціально значущі наслідки для енергетики, водопостачання, транспорту, охорони здоров'я та фінансових сервісів. Аналітичні огляди європейських інституцій фіксують у 2023–2024 рр. зростання складності атак, активну експлуатацію периферійних точок доступу та розширення векторів проникнення через хмарні й керовані сервіси. Для об'єктів КІ характерна одночасна присутність програм-вимагачів, деструктивного та шпигунського програмного забезпечення (ПЗ), атак через ланцюги постачання, DDoS-кампаній і цілеспрямованих операцій державного рівня, що корелюють із військово-політичними подіями та інформаційними впливами [1–3]. Для авіаційного сектора наслідком цього є ризик збоїв у системах обслуговування пасажирів і рейсів, інформаційного забезпечення, планування ресурсів та наземного обслуговування, а також у технологічних підсистемах аеропорту.

З позицій OT характер загроз деталізується в моделі MITRE ATT&CK for Industrial Control Systems (ICS), яка описує тактики та техніки впливу на контролери, інженерні робочі станції, PLC, HMI та промислові протоколи (Modbus, DNP3, IEC-104, OPC UA). Типовий сценарій передбачає початкову компрометацію IT-сегмента з подальшим горизонтальним переміщенням у бік OT-зони та втручанням у логіку технологічних процесів або спотворенням телеметрії й команд керування [4]. За даними ENISA, неадекватна сегментація та обмежена видимість у технологічних мережах призводять до тривалого перебування зловмисника в середовищі до моменту виявлення інциденту [1, 3].

Оперативні звіти спеціалізованих аналітичних центрів підтверджують стабільну активність OT-орієнтованих угруповань. Зокрема, у звітах компанії Dragos за 2024 рік, що є одним з визнаних світових лідерів у сфері промислової кібербезпеки, яка публікує звіт OT Cybersecurity: Year in Review, заснований на телеметрії з реальних промислових об'єктів та результатах реагування на інциденти, відзначено зростання кількості груп, що спеціалізуються на атаках проти енергетики, виробничих і телекомунікаційних секторів, із фокусом на компрометації віддаленого доступу, інструментів адміністрування та мережевих сервісів, включно з VPN-шлюзами [5, 6]. Це узгоджується з оцінками ENISA щодо ключової ролі периметрових сервісів і ланцюгів постачання як початкових векторів проникнення [1, 4].

В українському контексті звіти Держспецзв'язку та CERT-UA фіксують комплексні кампанії з використанням фішингу, шкідливих вкладень, деструктивного ПЗ, цілеспрямованих атак на державні реєстри та операторів КІ, а також DDoS-дії як інструмент відволікання та психологічного тиску [8–10].

Уразливості КІ значною мірою зумовлені історичними особливостями промислових систем. Багато протоколів ОТ були спроєктовані без сучасних механізмів автентифікації та шифрування, що в умовах конвергенції IT/OT, впровадження IoT і хмарних сервісів створює додаткові канали між сегментами. Рекомендації агентство з кібербезпеки та безпеки інфраструктури США CISA (Cybersecurity and Infrastructure Security Agency, для безпеки ICS акцентують необхідність жорсткої сегментації IT/OT, мінімізації прямих з'єднань, обов'язкового застосування багатофакторної автентифікації для віддаленого доступу, повної інвентаризації активів і відмови від довірених за замовчуванням сервісів [11–13].

Периферійні пристрої віддаленого доступу та інтернет-шлюзи залишаються критичним операційним ризиком через високу експонованість і регулярну появу уразливостей, що включаються до каталогу відомих уразливості, що використовуються (Known Exploited Vulnerabilities, KEV) агентства CISA. Регуляторні матеріали 2024–2025 рр. підкреслюють необхідність термінового усунення таких вад і визначають пріоритизацію виправлень за переліком KEV як базовий рівень кібергігієни для операторів КІ [15–18].

Окремий клас ризиків пов'язаний з атаками на ланцюги постачання, зокрема компрометацією бібліотек, оновлень ПЗ та сервісів керування третіх сторін. ENISA зазначає, що у 2023–2024 рр. ці атаки стали суттєвим джерелом початкового доступу, а в умовах КІ їхній вплив посилюється міжсекторальними залежностями. З огляду на обмеження повного патч-менеджменту в ОТ, стратегії пом'якшення мають включати ізоляційні контролі, моніторинг аномалій і аналіз трафіку [1, 2, 5, 11].

Програми-вимагачі, навіть без прямого шифрування ОТ-компонентів, суттєво впливають на безперервність критичних послуг через зупинки процесів і блокування диспетчерських IT-систем. [19–21].

У 2025 році, за оцінками ENISA, транспортний сектор ЄС, зокрема авіаційний транспорт і логістика, є другою за значимістю ціллю кіберзлочинців; при цьому концентрація інцидентів найбільшою мірою припадає на повітряний транспорт (58,4 %) та логістику (20,8 %), а суттєву частку становлять DDoS-атаки з боку хактивістів (87,6 %), тоді як кіберзлочини охоплюють 8,4 % усіх інцидентів і переважно представлені програмами-вимагачами (83,9 %) та витоками даних (16,1 %). Для галузі характерне поєднання атак на доступність (зокрема DDoS проти систем бронювання, вебресурсів аеропортів та авіакомпаній), загроз для даних (компрометація інформаційних систем управління рейсами, пасажирськими даними, вантажною логістикою), а також ризиків, пов'язаних із ланцюгами постачання IT-рішень для авіаційної сфери; з огляду на високу взаємозалежність авіатранспорту з іншими секторами (енергетика, цифрова інфраструктура, прикордонний контроль) саме цей сектор є одним із ключових з точки зору виникнення каскадних ефектів [14].

Фішинг і соціотехнічні методи залишаються основним механізмом первинної компрометації облікових записів із віддаленим доступом. Галузеві дослідження ICS/OT (SANS 2024) підкреслюють важливість захищеної архітектури, рольового контролю доступу, сегментації та багатофакторної автентифікації в поєднанні з ризик-орієнтованим управлінням уразливостями [22].

Нормативною основою управління вразливостями в промисловому середовищі є серія стандартів ISA/IEC 62443. Оновлена редакція 62443-2-1:2024 встановлює вимоги до програм безпеки власників IACS, що узгоджуються з принципами зонування, управління доступом, моніторингу та життєвого циклу змін, а технічні частини 62443-3-3 і 62443-4-2 формують практичну рамку зниження ризиків і пом'якшення наслідків інцидентів [23–25].

Практична реалізація зонально-канальної архітектури (IEC 62443) для ІКС авіаційної галузі передбачає логічне відокремлення IT-зони від технологічних сегментів ОТ та організацію контрольованих каналів взаємодії через DMZ (demilitarized zone, демілітаризована зона) із використанням шлюзів/проксі та журналюванням. Віддалений доступ до технологічних компонентів доцільно здійснювати виключно через керовані точки входу (VPN або bastion/jump host у DMZ) із MFA (multi-factor authentication, багатофакторна автентифікація), принципом найменших привілеїв, часовими політиками доступу та, за можливості, записом сесій для підвищення трасованості та можливостей розслідування інцидентів.

Таким чином, актуальний ландшафт загроз для КІ характеризується розрізненим ландшафтом загроз, атак через ланцюги постачання та експлуатацією уразливостей периферійних компонентів на тлі дефіциту сегментації й моніторингу в ОТ.

Для авіаційних суб'єктів КІ ці вектори загроз мають оцінюватися з урахуванням залежностей між ІКС аеропорту, авіакомпаній та суміжних

провайдерів, що включають в себе наземне обслуговування, постачальники сервісів, хмарні платформи, тощо.

Зниження ризику потребує переходу від суто реактивних заходів до системних профілактичних контролів, що охоплюють інвентаризацію активів, пріоритизацію усунення уразливостей за KEV, виявлення аномалій у ICS-протоколах і узгодження програм безпеки з вимогами IEC 62443 та рекомендаціями CISA/ENISA [11–13, 15, 23].

Зазначений ландшафт загроз і уразливостей критичної інфраструктури свідчить про обмежену ефективність виключно традиційних, переважно сигнатурних і реактивних механізмів кіберзахисту в умовах зростаючої складності IT/OT-середовищ. Багатовекторний характер атак, динаміка їх еволюції та вимоги до мінімізації часу виявлення інцидентів зумовлюють потребу у використанні підходів, здатних працювати з великими обсягами гетерогенних даних, виявляти нетипові поведінкові патерни та підтримувати обґрунтоване прийняття рішень у режимі, наближеному до реального часу. У цьому контексті особливої актуальності набувають інтелектуальні технології, що поєднують методи машинного навчання з формалізованими процесами управління ризиками та інженерними практиками безпечної експлуатації, адаптованими до специфіки критичної інфраструктури [35].

Обґрунтування доцільності застосування методів машинного навчання для оцінки ризиків об’єктів критичної інфраструктури для ІКС ЦА

Завдання оцінювання ризиків у критичній інфраструктурі доцільно формулювати як створення програмного модуля, здатного автоматично визначати рівень ризику на основі накопичених історичних даних. Такий підхід передбачає використання інформації з джерел CVE (Common Vulnerabilities and Exposures, публічний каталог ідентифікаторів уразливостей), журналів подій, записів інцидентів та телеметрії IT/OT, інтегруючи результати в процес управління ризиками відповідно до ISO/IEC 27005 [26] та забезпечуючи сумісність із специфічними вимогами IEC 62443-3-2 для IACS [26, 28]. Авторами досліджено ерспективи інтеграції машинного навчання для системи оцінки ризиків критичної інфраструктури в інформаційно-комунікаційних системах цивільної авіації [36, 37, 38].

У контексті управління ризиками оператор КІ розглядається, зокрема, аеропорт або авіакомпанія як власник/оператор ІКС де реалізовано:

- модель ризику, що включає активи, загрози, уразливості, сценарії та наслідки, відповідно до ISO/IEC 27005 і NIST SP 800-30. Для авіації до активів відносять як корпоративні сервіси й робочі станції, так і операційні компоненти (системи обслуговування рейсів/пасажирів) та OT-компоненти інженерної інфраструктури аеропорту [26, 28];
- встановлені критерії прийнятності ризику (наприклад, «низький», «помірний», «високий», «неприйнятний»);
- базовий реєстр ризиків та опис ключових критичних процесів і зон/каналів IT/OT згідно з IEC 62443-3-2. Доцільно фіксувати зони щонайменше рівня корпоративної IT-мережі, операційних сервісів, DMZ та OT-сегментів інженерних систем із визначеними каналами обміну. [27].

Програмний модуль у цій архітектурі виступає як «ризик-рушій» (risk engine), виконуючи такі функції:

1. Збір, нормалізація та обробка потоків даних із джерел безпеки, включно з SIEM/XDR журналами, мережевими метаданими, OT-телеметрією, системами управління вразливостями та каталогами CVE.
2. Формування ознак, релевантних для оцінки ризику.
3. Застосування методів машинного навчання для прогнозування ймовірності та потенційної інтенсивності небажаних подій щодо конкретних активів та сценаріїв.
4. Трансформація результатів ML-аналізу у ризик-скори та категорії ризику, узгоджені з визначеними критеріями прийнятності.
5. Інтеграція отриманих оцінок у реєстр ризиків та систему підтримки прийняття рішень, забезпечуючи оперативне інформування керівництва та можливість автоматизованого реагування.

Такий підхід дозволяє поєднати історичні дані, аналітичну потужність машинного навчання та формалізовані процеси управління ризиками, створюючи відтворювану та аудитоздатну систему для системного зниження ризиків у критичній інфраструктурі.

Формально розглядається множина активів $A = \{a_1, a_2, \dots, a_n\}$, множина сценаріїв загроз $S = \{s_1, s_2, \dots, s_n\}$, та часовий горизонт T(наприклад, місяць або квартал). Для кожної пари «актив–сценарій» (a_i, s_j) і періоду $t \in T$ необхідно отримати оцінку ризику за формулою 2.1:

$$R(a_i, s_j, t) = f(P_{inc}(a_i, s_j, t), C(a_i, s_j)), \qquad (1)$$

де $P_{inc}(a_i, s_j, t)$ – оцінена на основі даних і ML-моделей імовірність (або інтенсивність) реалізації небажаної події, $C(a_i, s_j)$ – міра наслідків (шкода для безперервності, безпеки, фінансів тощо), узгоджена з прийнятими у розділі 1 підходами до кількісного або комбінованого оцінювання ризику.

Для ІКС ЦА міра наслідків повинна відображати, зокрема, вплив на безперервність польотних операцій, обробку пасажирів і багажу, функції наземного забезпечення, а також на виконання вимог безпеки польотів і регуляторних процедур.

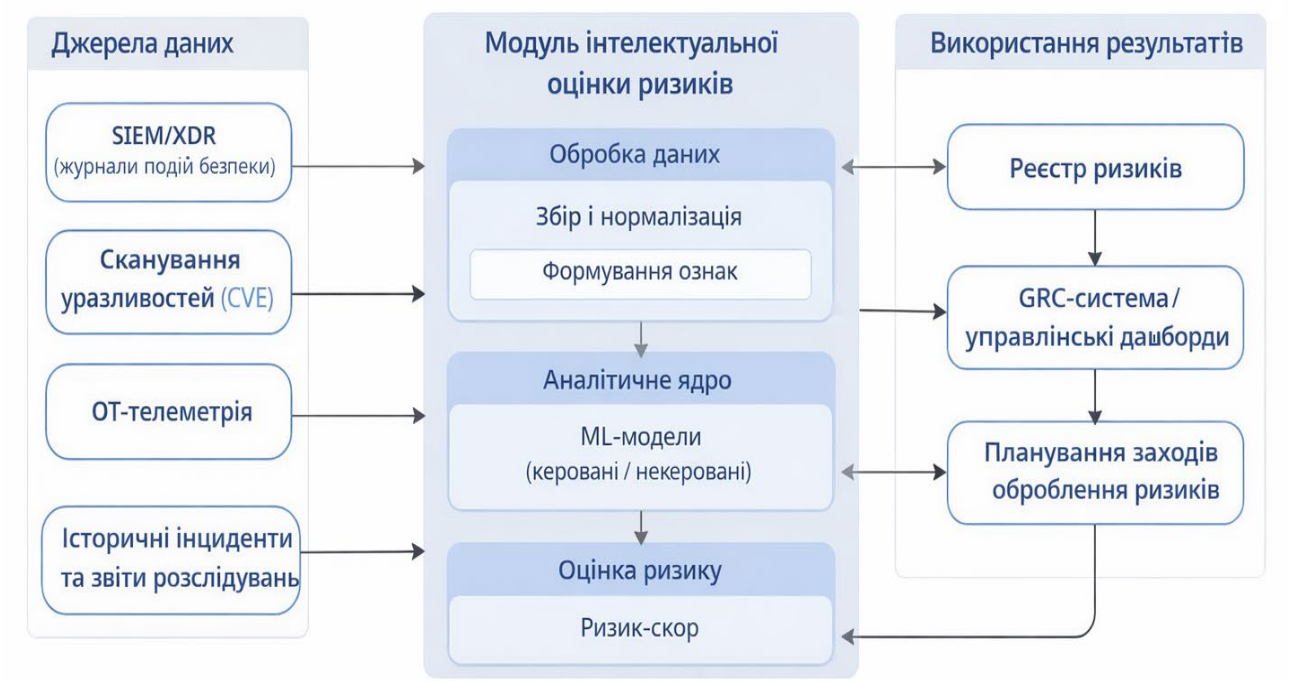
Метою застосування методів машинного навчання для оцінки ризиків об'єктів критичної інфраструктури є не заміна традиційного процесу оцінки ризиків, а його підсилення даними, що дозволяє зменшити суб'єктивність, скоротити час актуалізації оцінок і підвищити чутливість до нових патернів загроз та відхилень у поведінці IT/OT-систем. Основне завдання програмного модуля полягає у створенні керованого конвеєра, який забезпечує:

- побудову моделей на основі історичних інцидентів, CVE/KEV, журналів подій та операційних показників для прогнозування показників P_inc або обчислення ризик-скорів;
- перетворення результатів моделювання у формат, сумісний із реєстром ризиків та придатний для використання в процесах підтримки прийняття рішень, включно з плануванням заходів, вибором контролів та пріоритизацією інвестицій.

З огляду на особливості IT/OT-середовищ та характер наявних даних, застосовується гібридний підхід машинного навчання:

- некеровані алгоритми (кластеризація, виявлення аномалій, моделі щільності) аналізують події, виділяють типовий і нетиповий режим роботи, що дозволяє виявляти нові або рідко представлені сценарії;
- керовані моделі, навчені на історії інцидентів і підтверджених спрацюваннях, оцінюють ймовірність та/або очікувану тяжкість подій для відомих класів загроз;
- результати обох типів моделей об'єднуються у єдиний ризик-скор, який коригується відповідно до категорій ризику, визначених критеріями прийнятності ISO/IEC 27005 та IEC 62443-3-2 [28; 29].

Такий підхід забезпечує інтеграцію історичних даних, аналітики ML та формалізованих процесів управління ризиками, створюючи відтворювану і аудитоздатну основу для оцінки ризиків у критичній інфраструктурі (див. рис. 1).



ис. 1. Концептуальна схема інтеграції інтелектуальної оцінки ризиків із джерелами даних та системою підтримки прийняття рішень

Задача автоматизованого оцінювання ризиків у середовищах критичної інфраструктури характеризується низкою обмежень, що визначають вимоги до архітектури та алгоритмів програмного модуля. Насамперед, історичні дані про інциденти є неповними та суттєво незбалансованими: критичні події трапляються рідко, тоді як більшість спостережень відображає нормальні режими функціонування. Це зумовлює доцільність застосування методів машинного навчання, стійких до дисбалансу класів і здатних працювати з частковими даними [39].

Важливим обмеженням є необхідність узгодження роботи модуля з зонально-канальною архітектурою IT/OT та вимогами безпеки технологічних процесів. Оброблення інформації має здійснюватися з мінімальним впливом на продуктивні

середовища [25; 28]. Додатково, відповідно до регуляторних рамок NIS2, AI Act та NIST AI RMF, система повинна забезпечувати керованість життєвого циклу моделей, прозорість використаних даних і готовність до аудиту рішень [29, 30]. У мережах аеропортів та суміжних провайдерів типово реалізується зональний поділ із виділенням DMZ для інтеграційних сервісів та контрольованих каналів між IT і OT, що має враховуватися під час розміщення компонентів модуля та організації потоків даних.

На основі зазначеної постановки задачі сформовано вимоги до програмного модуля, які згруповано на функціональні, нефункціональні, вимоги до даних та інтеграційні вимоги.

До основних функціональних вимог належить збирання та узгодження даних про події безпеки, уразливості, конфігурацію активів і результати розслідувань інцидентів із різнорідних джерел (SIEM/XDR, OT-моніторинг, репозиторії уразливостей). Модуль повинен забезпечувати формування інформативних ознак, що відображають як статичний контекст активів (критичність, роль у технологічному процесі, рівень зони за IEC 62443), так і динамічну поведінку середовища (інтенсивність подій, зміни конфігурації, індикатори експлуатації уразливостей) [25; 27]. Критичною вимогою є трасованість результатів, тобто можливість відновлення зв'язку між оцінкою ризику, використаними даними та сформованими ознаками [28; 29].

Додатковими джерелами для авіаційних ІКС можуть виступати журнали операційних сервісів аеропорту, систем фізичного доступу, мережеві потоки в сегментах терміналів і телеметрія інженерних систем аеродрому.ML-компонент модуля має підтримувати як некеровані методи (виявлення аномалій, кластеризація), так і керовані моделі для оцінювання ймовірності або тяжкості інцидентів за наявності міток. Передбачається можливість перевчання, контролю версій і валідації моделей із використанням стандартних метрик якості (Precision, Recall, F1, PR-AUC, час до виявлення) [29]. Результати моделювання мають інтегруватися в узагальнений показник ризику $R(a_i, s_j, t)$ та відпо-відні категорії ризику згідно з підходами ISO/IEC 27005 і галузевих методик [26; 28; 30], з підтримкою агрегованого та деталізованого перегляду й експорту до реєстру ризиків (див. формулу 1).

До нефункціональних вимог належать вимоги до надійності, масштабованості та продуктивності. Модуль повинен забезпечувати періодичну переоцінку ризиків у прийнятні часові межі, залишаючись стійким до відмов і підтримуючи повернення до попередніх валідованих версій моделей. Окрему увагу приділено вимогам безпеки та відповідності: рольовий контроль доступу, захист каналів і сховищ даних, повне журналювання дій і змін моделей є необхідними для дотримання вимог ISO/IEC 27001, NIS2 та AI Act [29; 30].

В умовах критичної інфраструктури суттєве значення мають пояснюваність і аудитовність результатів. Модуль повинен надавати інтерпретовані пояснення оцінок ризику, зберігати стани моделей і даних для перевірок, а також підтримувати механізми людського нагляду для прийняття критичних рішень [27–30].

Вимоги до даних передбачають забезпечення їх цілісності, походження та якості, включно з розмежуванням навчальних і продуктивних наборів та виявленням дрейфу розподілів. Інтеграційні вимоги визначають взаємодію модуля з існуючими системами моніторингу, управління ризиками та підтримки управлінських рішень у межах процесів, визначених стандартом ISO/IEC 27005.

Вибір методів машинного навчання для оцінювання та прогнозування ризиків на прикладі авіаційної критичної інфраструктури

Сформульована задача передбачає побудову програмного модуля, здатного здійснювати оцінювання та прогнозування рівня ризику для комбінацій «актив – сценарій загрози» з використанням історичних даних про інциденти, телеметрії IT/OT-систем, відомостей про уразливості та результатів розслідувань. Особливості доступних даних – обмежена кількість прикладів, суттєвий дисбаланс класів, поєднання табличних і часових характеристик – у поєднанні з регуляторними вимогами до керованості та обґрунтованості моделей у секторах критичної інфраструктури [26, 30, 31] зумовлюють доцільність використання гібридного підходу, що поєднує методи класифікації, кластеризації, регресії та аномалієорієнтованого аналізу.

Узагальнено, дані для ML-компонента можна описати як множину спостережень

$$D = \{(x_k, y_k)\}_{k=1}^{N}, \qquad (2)$$

де $x_k \in R^d$ – вектор ознак, сформований на основі журналів подій, показників уразливостей, OT-телеметрії та контекстної інформації про актив і сценарій, а y_k — цільова змінна, як визначається постановкою задачі. Для класифікації вона відображає клас інциденту або категорію ризику, для регресії вона задається числовим показником, пов'язаним із ризиком, зокрема ймовірністю реа-

лізації сценарію, очікуваними втратами або інтенсивністю подій, для кластеризації та виявлення аномалій цільові мітки зазвичай відсутні, а структуру даних встановлюють методами некерованого навчання.

Для ІКС ЦА доцільно включати ознаки, що відображають критичність активу для процесів обслуговування рейсів і пасажирів. Важливо враховувати наявність підрядного або віддаленого доступу та залежності від третіх сторін. Окрему групу мають становити параметри технологічних підсистем аеродрому, зокрема електроживлення, освітлення та кліматичні системи.

Оскільки функція ризику (див. формулу 1) базується на оцінці імовірності або інтенсивності інциденту $P_{inc}(a_i, s_j, t)$ та величині наслідків $C(a_i, s_j)$, ML-моделі мають прямо або опосередковано апроксимувати ці складові. У простому випадку класифікаційна модель оцінює

$$P_{inc}(x) = g(x) \in [0; 1], \quad (3)$$

де $g(x)$ може реалізовуватися у вигляді логістичної регресії, ансамблів дерев рішень або градієнтного бустингу, а отримане значення використовується для обчислення ризик-скору. Альтернативно, регресійна модель.

$$R(x) = h(x). \quad (4)$$

З урахуванням NIST AI RMF та AI Act до IT/OT-застосувань, вибір алгоритмів обмежується методами, які поєднують достатню прогностичну здатність із контрольованістю, можливістю інтерпретації та підтримкою аудиту, а також забезпечують прозоре управління даними і життєвим циклом моделей. У межах запропонованого підходу виокремлюються три основні класи задач машинного навчання: класифікація, кластеризація (включно з виявленням аномалій) та регресія.

Керовані методи класифікації застосовуються для оцінювання ймовірності або категорії ризику за наявності хоча б обмеженого набору визначених та класифікованих інцидентів. У середовищах критичної інфраструктури це охоплює задачі бінарної та багатокласової класифікації (наприклад, за типами атак або рівнями ризику відповідно до критеріїв ISO/IEC 27005 та IEC 62443-3-2) [26; 27]. З огляду на дисбаланс класів і різнорідність ознак доцільним є використання алгоритмів, орієнтованих на табличні дані, зокрема логістичної регресії з регуляризацією, випадкових лісів і градієнтного бустингу. Ансамблеві методи забезпечують підвищену стійкість до шуму та нелінійностей і водночас дозволяють оцінювати внесок окремих ознак у прийняте рішення, що є важливим для інтерпретованості та аудиту [29; 32]. Якість таких моделей рекомендується оцінювати з використанням метрик Precision, Recall, F1 та PR-AUC, доповнюючи їх аналізом часу до виявлення інциденту [39].

Некеровані підходи відіграють важливу роль у ситуаціях дефіциту даних. Кластеризація дозволяє структурувати простір подій і активів, виділяючи групи з подібними профілями загроз, тоді як методи виявлення аномалій забезпечують ідентифікацію нетипових режимів роботи IT/OT-систем. Для цього можуть застосовуватися як класичні алгоритми (k-means, ієрархічна кластеризація, DBSCAN), так і підходи, орієнтовані на детекцію відхилень, зокрема Isolation Forest, One-Class SVM, LOF та автоенкодери, навчені на «нормальній» поведінці [32]. Порогові значення таких моделей можуть інтерпретуватися як індикатори підвищеного ризику або використовуватися як додаткові ознаки для керованих моделей. Водночас рекомендації ENISA та NCSC/CISA наголошують на необхідності контролю цих алгоритмів через ризики некоректного налаштування даних [33, 34].

Регресійні методи застосовуються для кількісного прогнозування ризику або його складових. До таких задач належать оцінювання очікуваної частоти інцидентів у сегменті, прогнозування можливих втрат або визначення часу до настання події. Залежно від характеру даних можуть використовуватися як лінійні регресійні моделі, так і ансамблеві підходи (random forest regressor, градієнтний бустинг), що добре працюють зі змішаними типами ознак і дозволяють аналізувати важливість факторів. Для часових рядів OT-параметрів і мережевих метрик можливе застосування ARIMA або рекурентних нейромереж, однак їх використання потребує додаткового обґрунтування з позицій інтепритованості та стійкості, визначених у NIST AI RMF та AI Act [29, 32].

Ключовим принципом запропонованого підходу є поєднання результатів різних класів моделей. Некеровані алгоритми використовуються для виявлення структур і формування додаткових індикаторів ризику, класифікаційні моделі – для оцінювання ймовірності реалізації конкретних сценаріїв, а регресійні – для обчислення узагальненого ризик-скору, сумісного з функцією $f(\cdot)$ у формулі 1. Об’єднання результатів може здійснюватися за допомогою ансамблювання або з урахуванням експертних коригувань для критичних рішень, що відповідає принципам багаторівневого контролю та захисту, сформульованим у NIST AI RMF, AI Act і рекомендаціях ENISA [29; 30].

Отже, вибір методів машинного навчання в програмному модулі базується на відповідності типу задачі, здатності працювати з гетерогенними та розбалансованими даними, дотриманні вимог

до аудиту, стійкості до зовнішніх впливів і можливості інтеграції в інформаційно-комунікаційні системи та мережі [29; 32–34].

Архітектура багаторівневої системи оцінки ризиків з інтеграцією методів машинного навчання

Сукупність функціональних вимог застосування гібридного підходу машинного навчання зумовлюють побудову багаторівневої архітектури, орієнтованої на керовану обробку даних і відтворюваність результатів. Архітектурне рішення має забезпечувати послідовний рух інформації від первинних джерел безпеки й операційної телеметрії до аналітичних моделей та подальшу інтеграцію результатів у реєстр ризиків і системи підтримки управлінських рішень, одночасно підтримуючи вимоги до керованості життєвого циклу моделей, прозорості та аудиту відповідно до ISO/IEC 27005, IEC 62443-3-2, NIST AI RMF і AI Act.

Узагальнено представлена багаторівнева система оцінки ризиків з інтеграцією методів машинного навчання у вигляді набору логічно відокремлених, але взаємопов'язаних підсистем, кожна з яких відповідає за окремий етап оброблення даних і формування оцінки ризику (рис. 2). Взаємодія між підсистемами здійснюється як через потоки даних, так і через керуючу інформацію, що забезпечує контроль, відтворюваність і можливість аудиту процесу оцінювання ризиків [39].

Підсистема збору даних забезпечує приймання й узгодження інформації з різнорідних IT/OT-джерел, виконуючи нормалізацію форматів, базову перевірку якості та, за потреби, первинні заходи з обмеження розкриття чутливих атрибутів. Оброблені записи передаються до централізованого сховища разом із метаданими, необхідними для простежуваності походження даних відповідно до вимог управління ризиками.

У авіаційних ІКС це охоплює події корпоративної мережі аеропорту/авіакомпанії, журнали операційних сервісів, телеметрію OT (інженерна інфраструктура) та сигнали засобів мережевої безпеки на межі зон і в DMZ.

Підсистема зберігання та управління даними виконує функції акумуляції аналітичних даних, підтримує семантичні представлення сутностей рівня «актив – сценарій – період» та забезпечує механізми відстеження походження і трансформацій інформації. Це створює основу для обґрунтованості результатів і подальшого аудиту ML-оцінок, що відповідає рекомендаціям ENISA та NCSC/CISA.

Підсистема формування ознак і підготовка наборів даних реалізуються як окремий рівень, на якому нормалізовані події та телеметрія перетворюються у вектори ознак, придатні для навчання і застосування моделей машинного навчання. Узгоджене зберігання визначень ознак забезпечує сталість між навчальними та продуктивними середовищами й підтримує керованість експериментів, як це передбачено NIST AI RMF.

Підсистема машинного навчання охоплює повний життєвий цикл моделей, починаючи з навчання й валідації до розгортання та моніторингу в експлуатації. Він підтримує різні типи моделей, контроль версій, оцінювання якості за погодженими метриками та виявлення деградації або дрейфу даних у часі. Засоби інтерпретації результатів забезпечують відповідність вимогам до прозорості й керованості високоризикових систем, визначеним у NIST AI RMF і AI Act.

Підсистема обчислення ризику реалізуються на рівні інтеграції аналітичних результатів, де виходи ML-моделей поєднуються з контекстною інформацією про активи, сценарії та наслідки для формування узагальненого ризик-скору і його відображення в прийнятій шкалі ризику. Отримані оцінки передаються до реєстру ризиків і суміжних систем управління через стандартизовані інтерфейси, що дозволяє вбудувати модуль у наявні процеси управління ризиками. У практичній постановці для авіації це дозволяє формувати ризик-скор як для IT-сервісів (операційні платформи, облікові записи), так і для OT-активів інженерної інфраструктури, пов'язуючи результати з конкретними процесами та SLA/BCP [34; 38].

Наскрізний рівень управління, безпеки та моніторингу забезпечує дотримання вимог інформаційної безпеки, відповідності та експлуатаційної надійності на всіх етапах роботи модуля. Він охоплює контроль доступу, журналювання, управління конфігураціями, спостереження за технічними показниками та якістю моделей, а також реалізацію заходів протидії загрозам, характерним для ML-систем, відповідно до рекомендацій ENISA, NCSC/CISA та MITRE ATLAS.

Запропонована архітектура забезпечує чітке розмежування функцій між компонентами, масштабованість окремих рівнів і відтворюваність процесів оцінювання ризиків, створюючи основу для безпечного та регуляторно узгодженого застосування методів машинного навчання в середовищах критичної інфраструктури.

Рис. 2. Багаторівнева система оцінки ризиків з інтеграцією методів машинного навчання

Далі важливим етапом є інтеграція програмного модуля оцінки ризиків у систему підтримки прийняття рішень та переведення результатів машинного аналізу з рівня аналітики у площину практичного управління. Ризик-скори для комбінацій «актив – сценарій – період» автоматично узгоджуються з реєстром ризиків, забезпечуючи його регулярне оновлення на основі фактичних даних відповідно до підходів ISO/IEC 27005 та IEC 62443. Відображенням цього є прийняття рішень у контексті безперервності польотних операцій, планів відновлення та регуляторної відповідності.

Через формалізовані пороги прийнятності оцінки ризику безпосередньо транслюються у керовані дії – ініціювання заходів з оброблення ризиків, запуск робочих процесів, підтримку рішень щодо змін архітектури захисту та розподілу ресурсів у GRC-середовищі. Результати модуля подаються у вигляді узгоджених дашбордів і звітів для оперативного, тактичного та стратегічного рівнів управління, що забезпечує єдине бачення ризик-профілю організації.

Оцінки ризику використовуються також для коригування пріоритетів реагування на інциденти та перегляду планів безперервності, а накопичені дані формують базу для аудитів і регуляторного контролю відповідно до вимог NIS2, CER і NIST. Реалізація зворотного зв’язку між прийнятими рішеннями та ML-моделями забезпечує адаптивність системи до зміни загроз, тоді як механізми людського нагляду гарантують контроль і відповідальність при ухваленні критичних рішень.

У результаті модуль оцінки ризиків інтегрується в цілісну процесну модель управління ризиками об’єктів критичної інфраструктури та підтримує прийняття рішень на всіх етапах життєвого циклу інциденту. Його вихідні показники використовують для формування пріоритетів моніторингу, вибору заходів захисту, планування реагування і контролю ефективності впроваджених рішень. В авіаційній галузі така інтеграція передбачає узгодження пріоритетів реагування з критичністю ключових сервісів терміналу й аеродрому, а також із операційними сценаріями, що впливають на безперервність надання послуг, безпеку наземних процесів і регулярність польотів. Оцінювання має враховувати взаємозалежності між цифровими сервісами, інженерною інфраструктурою та організаційними процесами, оскільки порушення в одному сегменті здатні каскадно позначатися на суміжних функціях і збільшувати сукупний ризик.

Висновки

У статті науково обґрунтовано теоретичний підхід до інтелектуалізованого оцінювання ризиків об'єктів критичної інфраструктури на основі методів машинного навчання з фокусом на авіаційну галузь та інформаційно-комунікаційні системи цивільної авіації. Показано, що конвергенція IT і OT у аеропортових і авіакомпанійних середовищах збільшує поверхню атак і підвищує критичність своєчасного виявлення загроз.

На основі аналізу актуального ландшафту загроз узагальнено ключові вектори ризику для ІКС авіаційної критичної інфраструктури. До них належать компрометація віддаленого доступу та периметрових сервісів, реалізація атак через ланцюги постачання, експлуатація відомих уразливостей з урахуванням пріоритизації за CISA KEV, а також обмеження патч-менеджменту в OT-сегментах. Отримані результати узгоджуються з оцінками ENISA для транспортного сектору, де авіація характеризується поєднанням атак на доступність (DDoS проти цифрових сервісів аеропортів і авіакомпаній) та кіберзлочинних сценаріїв, пов'язаних із програмами-вимагачами і компрометацією даних. Це підсилює аргументацію на користь пріоритетного зміцнення периметра та контрольованого віддаленого доступу, а також застосування підходу KEV для периметрових компонентів, які часто виступають стартовими точками проникнення до операційних і технологічних сегментів аеропортів, і вдосконалення процесів оновлення в середовищах з високими вимогами до безперервності.

Запропоновано концепцію багаторівневої системи оцінки ризиків, у якій програмний ML-модуль виконує роль аналітичного ядра та підтримує повний цикл обробки даних: збір і нормалізацію подій, формування ознак, навчання/валідацію моделей і генерацію ризик-оцінок для комбінацій «актив – сценарій загрози». Передбачено сумісність із зонально-канальною архітектурою IEC 62443 (сегментація, DMZ, контроль каналів взаємодії) та безпечним віддаленим доступом із MFA ознак.

Результати оцінювання інтегруються з SOC-процесами суб'єктів критичної інфраструктури, забезпечуючи ризик-орієнтовану пріоритизацію реагування, підтримку прийняття рішень щодо оброблення ризиків та підвищення трасованості й аудитоздатності.

Така інтеграція узгоджується з вимогами NIS2 та CER щодо управління ризиками, безперервності послуг і готовності до інцидентів. У результаті формується підстава для скорочення часу до виявлення та підвищення якості реагування саме у критичних для авіації ланках, починаючи з операційних сервісів до інженерної інфраструктури аеродрому.

Подальший розвиток підходу передбачає розширення модульної архітектури за рахунок кластеризаційних, аномалієорієнтованих і регресійних методів, а також поглиблення набору ознак (зокрема показники експлуатації уразливостей, наявність публічних патчів, часові характеристики та індикатори реальної активності атак) для підвищення точності й оперативності оцінювання ризиків у ІКС авіаційної критичної інфраструктури.

ЛІТЕРАТУРА

[1] ENISA. ENISA Threat Landscape 2024 (July 2023 – June 2024). URL: https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf (access data 25.01.2026)

[2] ENISA. ENISA Threat Landscape 2023. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%2023.pdf (access data 25.01.2026)

[3] ENISA. Threat Landscape – overview page (ETL 2024 briefing). URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (access data 25.01.2026)

[4] MITRE. ATT&CK® for ICS Matrix. URL: https://attack.mitre.org/matrices/ics/ (access data 25.01.2026)

[5] Dragos. OT Cybersecurity Year in Review (огляд звіту за 2024 рік). URL: https://www.dragos.com/ot-cybersecurity-year-in-review (access data 25.01.2026)

[6] Dragos. 2025 OT Cybersecurity Year in Review – PDF. URL: https://pkcert.gov.pk/uploads/2025/02/Dragos-2025-OT-Cybersecurity-Report-A-Year-in-Review.pdf (access data 25.01.2026)

[7] FBI/IC3. Russian Military Cyber Actors Target U.S. and Global Networks (CSA, 05.09.2024). URL: https://www.ic3.gov/CSA/2024/240905.pdf (access data 25.01.2026)

[8] State Cyber Protection Centre (SCPC, Держспецзв'язку). Annual Report 2024. URL: https://scpc.gov.ua/api/files/4560c0ba-c6c0-4935-b48d-0232dd659df3 (access data 28.01.2026)

[9] Держспецзв'язку / CERT-UA. Аналітика CERT-UA (огляд тенденцій, 30.09.2025). URL: https://cip.gov.ua/ua/filter?tagId=68851 (access data 28.01.2026)

[10] РНБО України. Огляд подій у сфері кібербезпеки (січень 2024). URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/Cyber%20digest/Cyber%20digest_Jan_2024_UA.pdf (access data 28.01.2026)

[11] CISA. Cybersecurity Best Practices for Industrial Control Systems (ICS). URL: https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf (access data 28.01.2026)
[12] CISA. Primary Mitigations to Reduce Cyber Threats to Operational Technology. URL: https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology (access data 28.01.2026)
[13] CISA. Foundations for OT Cybersecurity: Asset Inventory Guidance URL: https://www.cisa.gov/resources-tools/resources/foundations-ot-cybersecurity-asset-inventory-guidance-owners-and-operators (access data 01.02.2026)
[14] ENISA. ENISA Threat Landscape 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025. (access data 01.02.2026)
[15] CISA. Known Exploited Vulnerabilities (KEV) Catalog. URL: https://www.cisa.gov/known-exploited-vulnerabilities-catalog (access data 01.02.2026)
[16] CISA. Advisory: Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b (access data 01.02.2026)
[17] CISA. Emergency Directive ED 24-01 щодо Ivanti URL: https://www.cisa.gov/news-events/directives/ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities (access data 01.02.2026)
[18] CISA. Cross-Sector Cybersecurity Performance Goals (оглядова сторінка). URL: https://www.cisa.gov/cross-sector-cybersecurity-performance-goals (access data 01.02.2026)
[19] GAO. Critical Infrastructure: Ransomware Impacts (GAO-24-106221, 30.01.2024). URL: https://www.gao.gov/assets/gao-24-106221.pdf
[20] CISA. StopRansomware – Black Basta URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a (access data 01.02.2026)
[21] DNI/CTIIC. Worldwide Ransomware Attacks as of June 2024 URL: https://www.dni.gov/files/CTIIC/documents/products/Worldwide_Ransomware_Attacks_as_of_June_2024_Consistent_With_Previous_Year_Sep2024.pdf (access data 01.02.2026)
[22] SANS Institute. The 2024 State of ICS/OT Cybersecurity URL: https://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity (access data 01.02.2026)
[23] IEC. IEC 62443-2-1:2024 – Security program requirements for IACS asset owners (офіційна сторінка). URL: https://webstore.iec.ch/en/publication/62883 (access data 01.02.2026)
[24] IEC. IEC 62443-3-3:2013 – System security requirements and security levels (офіційна сторінка). URL: https://webstore.iec.ch/en/publication/7033 (access data 01.02.2026)
[25] ISA/ISAGCA. ISA/IEC 62443 Series of Standards – огляд. URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (access data 05.02.2026)
[26] ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks. Geneva: ISO/IEC, 2022. URL: https://www.iso.org/standard/80585.html (access data 05.02.2026)
[27] IEC 62443-3-2:2020 – Security for industrial automation and control systems – Part 3–2: Security risk assessment for system design. Geneva: IEC, 2020. URL: https://webstore.iec.ch/en/publication/30727 (access data 05.02.2026)
[28] NIST. SP 800-30 Rev.1: Guide for Conducting Risk Assessments. Gaithersburg, MD: NIST, 2012. URL: https://csrc.nist.gov/pubs/sp/800/30/r1/final (access data 05.02.2026)
[29] NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg, MD: NIST, 2023. URL: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf (access data 05.02.2026)
[30] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689, URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (access data 05.02.2026)
[31] IEC 31010:2019 – Risk management – Risk assessment techniques. Geneva: ISO/IEC, 2019. URL: https://www.iso.org/standard/72140.html (access data 05.02.2026)
[32] ENISA. Securing Machine Learning Algorithms. Athens: European Union Agency for Cybersecurity, 2021. URL: https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms (access data 05.02.2026)
[33] NCSC-UK; CISA та ін. Guidelines for Secure AI System Development. 2023 (оновлення 2024). URL: https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf (access data 05.02.2026)
[34] MITRE. ATLAS – Adversarial Threat Landscape for Artificial-Intelligence Systems (офіційний сайт). URL: https://atlas.mitre.org/ (access data 05.02.2026)
[35] Ільєнко А.В., Телющенко В. А., Дубчак О. А. Сучасні кіберзагрози критичної інфраструктури України та світу // Кібербезпека: освіта, наука, техніка. 2025. Т. 3, № 27. С. 150–164. https://doi.org/10.28925/2663-4023.2023.27.719
[36] Анна Ільєнко, Валентина Телющенко. Методи оцінювання ризиків кіберзагроз у критичній інфраструктурі: тез доп., VIII міжнародна науково-практична конференція: Проблеми кібербезпеки інформаційно-комунікаційних систем

(PCSICS), м. Київ, 21 квітня 2025 року. К.: ВПЦ «Київський університет», 2025. С. 52-53.
[37] Телющенко В. А., Ільєнко А. В. Перспективи інтеграції машинного навчання для системи оцінки ризиків критичної інфраструктури // Проблеми кібербезпеки інформаційно-комунікаційних систем: VIII міжнар. наук.-практ. конф., 11 квітня 2025 р. Київ, 2025. С. 52–53.
[38] Ільєнко А. В., Телющенко В. А. Методика ранжування підходів до оцінки кіберризиків в інформаційно-комунікаційних системах цивільної авіації // Резильєнтність динамічних систем : матеріали III наук.-практ. конф. Ін-ту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України (Київ, 06 листопада 2025 р.). Київ : ІПМЕ ім. Г. Є. Пухова НАН України, 2025. С. 124–127.
[39] Ільєнко А. В., Телющенко В. А. Методи оцінювання ризиків кіберзагрозв інформаційно-комунікаційних системах об'єктів цивільної авіації. (2025). Безпека інформаційних систем і технологій, 2(10). С. 5–15.

Ільєнко А. В., Ільєнко С. С., Телющенко В. А., Маляренко С. Д.

ТЕОРЕТИЧНИЙ ПІДХІД ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ОЦІНКИ РИЗИКІВ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Актуальність дослідження зумовлена зростанням кіберзагроз для об'єктів критичної інфраструктури на тлі конвергенції інформаційних і операційних технологій та збільшення поверхні атак через хмарні сервіси, віддалений доступ і ланцюги постачання. Для цивільної авіації ці тенденції є особливо чутливими, оскільки порушення працездатності інформаційно-комунікаційних систем здатне впливати на регулярність рейсів, наземні процеси, сервіс пасажирів і стійкість аеропортової інженерної інфраструктури.

Проблема полягає у недостатній ефективності суто реактивних підходів до управління ризиками, обмеженій видимості подій у технологічних сегментах і складності оперативної пріоритизації інцидентів. Метою статті є наукове обґрунтування підходу до інтелектуалізованого оцінювання ризиків із застосуванням методів машинного навчання, орієнтованого на підвищення своєчасності виявлення загроз і ефективності реагування з урахуванням вимог NIS2 та CER і галузевих рекомендацій. Як шлях вирішення запропоновано процесно-орієнтовану модель, у якій машинне навчання інтегрується з підходами ISO IEC 27005, NIST SP 800-30 та принципами зонально-канальної архітектури IEC 62443. У роботі узагальнено ландшафт загроз для критичної інфраструктури та авіаційного сектора, зокрема ризики компрометації віддаленого доступу, атаки через ланцюги постачання та експлуатацію відомих уразливостей із пріоритизацією за KEV.

Обґрунтовано використання гібридного набору методів машинного навчання, який поєднує класифікацію, регресію, кластеризацію та виявлення аномалій, а також визначено підхід до формування ознак на основі журналів подій, показників уразливостей, OT-телеметрії та контексту критичності активів аеропорту й авіакомпанії. Результатом є концепція багаторівневої архітектури системи оцінки ризиків, що охоплює збір і нормалізацію даних, формування ознак, керований життєвий цикл моделей і інтеграцію ризик-оцінок із SOC-процесами та реєстром ризиків. У висновках показано, що запропонований підхід створює відтворювану та аудитоздатну основу для ризик-орієнтованої пріоритизації реагування в ІКС цивільної авіації, а також визначено напрями подальшого розвитку за рахунок розширення набору ознак і модулів аналітики.

Ключові слова: ризики; кібербезпека, критична інфраструктура; цивільна авіація; ІКС; ОТ; машинне навчання; SOC; IEC 62443; NIS2; CVE.

Ilienko A., Ilienko S., Teliushchenko V., Malyarenko S.

THEORETICAL APPROACH TO THE APPLICATION OF MACHINE LEARNING METHODS FOR ASSESSING THE RISKS OF CRITICAL INFRASTRUCTURE FACILITIES

The relevance of this study is driven by the growing cyber threat landscape affecting critical infrastructure amid the convergence of information technology and operational technology and the expansion of attack surfaces through cloud services, remote access, and supply chains. In civil aviation, these challenges are particularly sensitive because disruptions in information and communication systems may affect flight regularity, ground operations, passenger services, and the resilience of airport engineering infrastructure.

The problem addressed in the paper is the limited effectiveness of purely reactive risk management, insufficient visibility in technological networks, and the difficulty of timely incident prioritization. The purpose of the article is to substantiate an intellectualized cyber risk assessment approach based on machine learning to improve detection timeliness and response effectiveness while aligning with NIS2 and CER requirements and sector-specific guidance. The proposed solution is a process-oriented model in which machine learning is integrated with ISO IEC 27005, NIST SP

800-30, and the zone-and-conduit principles of IEC 62443. The paper summarizes key threat vectors relevant to critical infrastructure and aviation, including remote access compromise, supply chain attacks, and exploitation of known vulnerabilities with mitigation prioritization guided by the KEV catalog.

A hybrid machine learning strategy is justified by combining classification, regression, clustering, and anomaly detection, along with a feature engineering approach that leverages security logs, vulnerability indicators, OT telemetry, and asset criticality context for airports and airlines. The main result is a concept of a multi-layer risk assessment architecture covering data collection and normalization, feature generation, controlled model lifecycle management, and integration of risk outputs with SOC processes and the risk register. The conclusions demonstrate that the approach provides a reproducible and auditable basis for risk-driven response prioritization in civil aviation information and communication systems and outlines directions for further enhancement through richer feature sets and analytical modules

Keywords: risk; cybersecurty. critical infrastructure; civil aviation; ICT; OT; machine learning; SOC; IEC 62443; NIS2; CVE

Дата першого надходження: 10.02.2026 р.
Дата прийняття до друку: 10.03.2026 р.
Дата публікації: 27.04.2026 р.