https://doi.org/10.31891/2307-5732-2026-365-57
УДК 004.056

ІЛЬЄНКО АННА
Державний університет «Київський авіаційний інститут»
ORCID https://orcid.org/0000-0001-8565-1117
e-mail: anna.ilienko@npp.kai.edu.ua
ІЛЬЄНКО СЕРГІЙ
Державний університет «Київський авіаційний інститут»
ORCID https://orcid.org/0000-0002-0437-0995
e-mail: serhii.ilienko@npp.kai.edu.ua
ГАЛИЧ ЄВГЕНІЯ
Державний університет «Київський авіаційний інститут»
ORCID https://orcid.org/0009-0008-2610-1439
e-mail: 7405781@stud.kai.edu.ua
ПАВЛЕНКО ВЛАДИСЛАВ
Державний університет «Київський авіаційний інститут»
ORCID https://orcid.org/0009-0008-8072-5525
e-mail: 7328430@stud.kai.edu.ua

МЕТОДОЛОГІЧНІ ЗАСАДИ СТВОРЕННЯ СТРУКТУРНО-ФУНКЦІОНАЛЬНОЇ МОДЕЛІ СПЕЦІАЛІЗОВАНИХ SOC-ЦЕНТРІВ ДЛЯ СУБ'ЄКТІВ АВІАЦІЙНОЇ ДІЯЛЬНОСТІ УКРАЇНИ

Стаття присвячена дослідженню ролі Security Operations Center (SOC) як організаційно-операційного механізму забезпечення кіберстійкості суб'єктів цивільної авіації. Актуальність теми зумовлена високим рівнем цифровізації авіаційної галузі, інтеграцією інформаційних і технологічних систем та зростанням кількості кіберзагроз, що можуть впливати на безперервність функціонування критичної авіаційної інфраструктури.

У роботі проаналізовано сучасні підходи до організації центрів моніторингу та реагування на кіберінциденти, розглянуто концептуальні засади функціонування SOC у системі кібербезпеки та їх роль у забезпеченні безперервного моніторингу подій інформаційної безпеки, виявлення та реагування на кіберінциденти. Проведено аналіз світової практики створення та функціонування SOC на об'єктах критичної інфраструктури цивільній авіації. Визначено типові організаційні моделі, функціональні завдання та особливості їх впровадження в інфраструктурі аеропортів, що сертифіковані за міжнародним законодавством (ICAO).

На основі аналізу міжнародного досвіду, нормативних вимог Європейського Союзу та національного законодавства України обґрунтовано необхідність створення спеціалізованих SOC для суб'єктів авіаційної діяльності як складової системи забезпечення кіберстійкості критичної інфраструктури. Запропоновано структурно-функціональну модель SOC сертифікованого ICAO аеропорту, що забезпечує централізований моніторинг подій інформаційної безпеки в IT та OT середовищах, аналіз кіберінцидентів, координацію реагування та інтеграцію результатів до системи управління ризиками. Також сформовано методологічні засади побудови та впровадження SOC, які передбачають формування операційного контуру моніторингу, аналітичної спроможності, процедур реагування та взаємодії з національною системою реагування на кіберінциденти.

Практична доцільність дослідження полягає у формуванні концептуальних підходів до створення SOC для суб'єктів авіаційної діяльності України, що дозволяє підвищити ефективність виявлення та реагування на кіберінциденти, забезпечити інтеграцію аеропортів до національної системи кібербезпеки та підвищити рівень кіберстійкості критичної інфраструктури цивільної авіації.

Ключові слова: *Security Operations Center, кіберстійкість, цивільна авіації, критична інфраструктура, моніторинг безпеки, кіберризики.*

ANNA ILIENKO, SERHII ILIENKO, YEVHENIIA HALYCH, VLADYSLAV PAVLENKO
State University "Kyiv Aviation Institute"

METHODOLOGICAL PRINCIPLES OF CREATING A STRUCTURAL-FUNCTIONAL MODEL OF SPECIALIZED SOC-CENTERS FOR AVIATION ENTITIES OF UKRAINE

The article is devoted to the study of the role of the Security Operations Center (SOC) as an organizational and operational mechanism for ensuring cyber resilience of civil aviation entities. The relevance of the topic is due to the high level of digitalization of the aviation industry, the integration of information and technological systems and the increase in the number of cyber threats that can affect the continuity of the functioning of critical aviation infrastructure.

The paper analyzes modern approaches to the organization of monitoring and response centers for cyber incidents, considers the conceptual principles of the functioning of SOC in the cybersecurity system and their role in ensuring continuous monitoring of information security events, detection and response to cyber incidents. An analysis of the world practice of creating and operating SOCs at critical civil aviation infrastructure facilities is conducted. Typical organizational models, functional tasks and features of their implementation in the infrastructure of airports certified under international law (ICAO) are identified.

Based on the analysis of international experience, regulatory requirements of the European Union and national legislation of Ukraine, the need to create specialized SOCs for aviation entities as a component of the system for ensuring cyber resilience of critical infrastructure is substantiated. A structural and functional model of the SOC of an ICAO-certified airport is proposed, which provides centralized monitoring of information security events in IT and OT environments, analysis of cyber incidents, coordination of response and integration of results into the risk management system. Methodological principles for the construction and implementation of SOCs are also formed, which provide for the formation of an operational monitoring circuit, analytical capabilities, response procedures and interaction with the national cyber incident response system.

The practical feasibility of the study lies in the formation of conceptual approaches to the creation of SOC for aviation entities in Ukraine, which allows to increase the efficiency of detecting and responding to cyber incidents, ensure the integration of airports into the national cybersecurity system, and increase the level of cyber resilience of critical civil aviation infrastructure.

Keywords: *Security Operations Center, cyber resilience, civil aviation, critical infrastructure, security monitoring, cyber risks.*

Стаття надійшла до редакції / Received 11.02.2026
Прийнята до друку / Accepted 11.03.2026
Опубліковано / Published 28.05.2026

Постановка проблеми

Цивільна авіація та її складові, зокрема сертифіковані ICAO аеропорти у нормативно-правовому полі Європейського Союзу віднесені до сектору з високою критичністю. Відповідно до Директиви (ЄС) 2022/2555 (NIS2), авіаційний транспорт включений до переліку секторів критичної інфраструктури, для яких встановлюються підвищені вимоги щодо кібербезпеки та стійкості мережевих і інформаційних систем. Дана класифікація показує важливіть забезпечення кіберстійкості та безперервності функціонування всіх систем авіації, своєчасного виявлення кіберінцидентів та мінімізації їх впливу на операційну діяльність [1].

Сучасні суб'єкти авіаційної діяності функціонують як складні інформаційно-комунікаційні системи, у межах яких інтегруються автоматизовані системи управління повітряним рухом (ATC/ATM), аеропортові та аеродромні енергосистеми (системи електропостачання), аеронавігаційні системи та системи автоматичної посадки (ILS, GLS), метеорологічні станції, аеропортові операційні інформаційні платформи, системи обробки даних про пасажирів та їх багажу, корпоративні IT-мережі та хмарні сервіси (пікреслено для формули). Порушення роботи одного з цифрових сервісів аеропорту може призводити до серйозних порушень, які впливають на операційну діяльність, координацію процесів та здатність своєчасно реагувати на інциденти.

Цифровізація авіаційної діяльності підвищує ефективність управління, але часті кібератаки ускладнюють забезпечення безперервності функціонування критичних сервісів. За результатами аналізу кіберзагроз за період 2024-2025 років авіаційний сектор є вразливим до атак типу ransomware, компрометації ланцюгів постачання програмного забезпечення, а також зловмисного використання легітимних облікових записів з подальшим розвитком атаки у внутрішніх мережах організації (з стійким збільшенням та розвитком) [2]. Звіт ENISA вказує, що для авіаційної галузі особливо небезпечними є атаки, спрямовані на порушення доступності операційних та інформаційних систем аеропортів, а також інциденти на стику IT- та OT-середовищ, які можуть мати серйозний вплив на операційну діяльність і вимагати переходу до ручного управління [3].

Традиційні підходи до кіберзахисту систем ґрунтуються на обов'язкових періодичних перевірках. Проте з огляду на цілодобову роботу аеропортових інформаційно-комунікаційних систем цього недостатньо. Для максимального захисту критичних систем Регуляторна рамка Part-IS, встановлена Commission Implementing Regulation (EU) 2023/203, зобов'язує авіаційні організації впровадити та підтримувати систему управління інформаційною безпекою (СУІБ), що включає заходи з виявлення подій інформаційної безпеки, ідентифікації інцидентів із потенційним впливом на безпеку польотів та авіаційну безпеку з реагуванням та відновлення після інцидентів [4]. Згідно рекомендацій Part-IS організації мають оперативно повідомляти про інциденти та вміти виявляти, відповідати та відновлювати систему у визначений термін. Процес управління кіберінцидентами має забезпечувати безперервний моніторинг та удосконалювати заходи у відповідь на інцидент.

У міжнародній практиці цивільної авіації зафіксовано тенденцію впровадження Security Operations Center (SOC) як спеціалізованих центрів моніторингу, аналізу та реагування на кіберінциденти в сертифікованих міжнародних аеропортах. Для України питання створення спеціалізованих аеропортових SOC-центрів є особливо актуальним з огляду на належність об'єктів цивільної авіації до критичної інфраструктури держави та необхідність їх інтеграції у національну систему реагування на кіберінциденти. У цьому контексті важливою є взаємодія спеціалізованих аеропортових SOC-центрів з урядовою командою реагування CERT-UA, що дозволить забезпечити координацію дій, обмін інформацією про загрози та своєчасну реакцію на інциденти.

Аналіз останніх джерел

Security Operations Center (SOC) у сучасній практиці кібербезпеки розглядається як організаційно-функціональний центр, відповідальний за централізований постійний моніторинг, аналіз подій інформаційної безпеки, управління кіберінцидентами та координацію реагування на них у режимі, наближеному до реального часу. Метою SOC-центру є визначення ситуаційної обізнаності стану систем безпеки і забезпечення захисту мереж критичної інфраструктури. У прикладному розумінні SOC-центр розглядається не лише як організаційний підрозділ, а як поєднання кваліфікованого персоналу, процесів та технологій, необхідних для забезпечення безперебійного контролю кібербезпеки, визначені процедури реагування та обробки інцидентів, технічні засоби збору і кореляції подій, що дозволяє своєчасно виявляти та обробляти кіберінциденти [5,7].

Важливою характеристикою SOC-центру є його централізований та організаційний характер, що функціонує як структурна одиниця, відповідальна за координацію дій у сфері кібербезпеки на рівні всієї організації та є підрозділом, який забезпечує узгоджене управління процесами виявлення загроз, аналізу подій та реагування на інциденти [6]. SOC-центр функціонує безперервно, а аналітики здійснюють постійний моніторинг інформаційних систем, аналізують події безпеки та координують реагування на інциденти у реальному часі. Такий підхід забезпечує функціональні перевагами таких спеціалізованих SOC-центрів: скорочення часу між

виникненням інциденту та початком реагування, що є критично важливим для забезпечення кіберстійкості; забезпечення концентрації інформації про події безпеки з різних сегментів інформаційної інфраструктури; узагальнення даних та виконання функції вузла ситуаційної обізнаності, який дозволяє своєчасно оцінювати ризики, визначати пріоритети реагування та координувати дії відповідальних підрозділів; централізація операцій кібербезпеки як ключовий чинник підвищення ефективності реагування на кіберінциденти та підвищення кіберстійкості критичної інфраструктури. На відміну від традиційного підходу до кібербезпеки, який орієнтований переважно на запобігання інцидентам, концепція кіберстійкості спеціалізованих SOC-центрів охоплює повний життєвий цикл кіберінциденту, включно з фазами виявлення, реагування та відновлення [7,8].

Забезпечення кіберстійкості реалізується у міжнародній практиці через процесно-орієнтовані моделі управління кіберризиками. Базовою моделю такого типу є NIST Cybersecurity Framework, у межах якої визначено п'ять взаємопов'язаних функцій: Identify (ідентифікація активів, загроз і ризиків), Protect (захист та впровадження запобіжних заходів), Detect (виявлення кіберінцидентів та аномалій), Respond (реагування на інциденти та мінімізація наслідків), Recover (відновлення функціонування та забезпечення безперервності діяльності). Дана рамкова політика кібербезпеки покращення безпеки критичної інфраструктури підкреслює, що забезпечення стійкості інформаційних систем до кіберзагроз неможливе без впроваджених механізмів безперебійного виявлення подій безпеки, організованого реагування на інциденти та відновлення критичних функцій. Саме централізація операційних процесів управління інцидентами дозволяє скоротити час виявлення загроз, мінімізувати їх наслідки та забезпечити швидке відновлення функціонування функціональних систем та обладнання після кібератак [9].

Формулювання цілей

Метою статті є обґрунтування необхідності створення спеціалізованих центрів моніторингу та реагування на кіберінциденти (Security Operations Center, SOC) для суб'єктів авіаційної діяльності як організаційного механізму забезпечення кіберстійкості критичної авіаційної інфраструктури. Досягнення цієї мети передбачає комплексний аналіз концепції функціонування SOC-центрів у системі кібербезпеки критичної авіаційної інфраструктури, дослідження світового досвіду їх впровадження в цивільній авіації, вивчення міжнародних нормативних вимог щодо кіберстійкості авіаційної галузі, а також визначення концептуальних засад формування структурно-функціональної моделі SOC-центрів для суб'єктів авіаційної діяльності України.

У межах дослідження передбачається аналіз ролі SOC-центрів як централізованого операційного механізму безперервного моніторингу подій інформаційної безпеки, виявлення та аналізу кіберінцидентів, координації реагування та інтеграції результатів інцидентів до системи управління безпекою і кіберризиками. Окрема увага приділяється узагальненню світової практики створення SOC-центрів у провідних сертифікованих ICAO міжнародних аеропортах України, аналізу та визначенню їх організаційних моделей та функціональних характеристик. На основі поєднання міжнародного досвіду, нормативно-правових вимог Європейського Союзу та національного законодавства України у статті планується розробити концептуальні засади побудови SOC для субєктів авіаційної діяльності України, запропонувати структурно-функціональну модель такого центру та визначити методологічну послідовність його створення й впровадження в системі управління кібербезпекою суб'єктів авіаційної діяльності.

Виклад основного матеріалу

Цивільна авіація належить до секторів критичної інфраструктури, оскільки забезпечує безперервність транспортних, економічних та соціальних процесів на національному й міжнародному рівнях. Будь-яке порушення безпеки та/або доступності її інформаційно-комунікаційних систем може мати значний вплив на функціонування міжнародного повітряного сполучення. У зв'язку з цим питання кібербезпеки цивільної авіації винесено на рівень міжнародного регулювання. У Резолюції ICAO A40-10 *"Addressing Cybersecurity in Civil Aviation"* кіберзагрози визначено як фактор, що впливає на безпеку та безперервність функціонування міжнародної цивільної авіації. Документ рекомендує державам розробляти національні політики кібербезпеки, інтегрувати кіберзахист у систему авіаційної безпеки, а також розвивати спроможності щодо запобігання, виявлення та реагування на кіберінциденти. При цьому акцентується перехід від традиційного підходу захисту до концепції кіберстійкості, що передбачає здатність систем протидіяти загрозам, реагувати на інциденти та відновлювати функціонування після їх виникнення [18]. На рівні Європейського Союзу обов'язкові вимоги до кібербезпеки суб'єктів цивільної авіації визначені Commission Delegated Regulation (EU) 2022/1645, який передбачає впровадження системи управління інформаційною безпекою, інтегрованої до загальної системи управління безпекою організації. Регламент встановлює необхідність ідентифікації та оцінювання ризиків інформаційної безпеки, впровадження заходів контролю, постійного моніторингу загроз, виявлення інцидентів і реалізації процедур реагування, що фактично формує повний цикл управління кіберінцидентами – від запобігання до відновлення. Практичні рекомендації щодо організації таких механізмів надає **ENISA**, зокрема у документі *"How to set up CSIRT and SOC"*, де визначено функціональні завдання, організаційні моделі та ресурсні вимоги до центрів реагування на інциденти та операційних центрів безпеки [19].

Отже, міжнародні та європейські нормативні документи формують комплексну основу забезпечення кіберстійкості цивільної авіації як сектору критичної інфраструктури: ICAO визначає стратегічні напрями розвитку спроможностей, Regulation (EU) 2022/1645 встановлює обов'язкові процесні вимоги, а ENISA надає методичні рекомендації щодо їх практичної реалізації.

Аналіз світової практики створення та функціонування Security Operations Center у цивільній авіації

Світова практика розвитку цивільної авіації вже має приклади впровадження у провідних міжнародних сертифікованих ICAO аеропортах SOC-центрів як організаційної форми централізованого моніторингу подій безпеки та управління кіберінцидентами. Такі застосування вже не розглядаються як допоміжні IT-підрозділи, а виступають складовими системи забезпечення кіберстійкості та безперервності операційної діяльності.

Приклади:

1. Цілодобовий спеціалізований SOC-центр аеропорту Sydney Airport (Австралія). Створено централізований механізм безперервного моніторингу подій інформаційної безпеки та реагування на кіберзагрози. Впровадження здійснювалося у співпраці з урядом Австралії та передбачало поступове нарощування спроможностей із використанням керованих сервісів управління кіберризиками [10].

2. Спеціалізована внутрішня модель SOC-центру аеропорту Vaclav Havel Airport Prague (Чехія) для захисту стратегічної інфраструктури аеропорту. Забезпечується багаторівневий моніторинг виявлення/ блокування загроз, використовується штучний інтелект, біометричні та автоматизовані засоби аналізу загроз [11].

3. Модель Managed SOC- центру аеропорту Stuttgart Airport (Німеччина) експлуатується зовнішнім провайдером. Центр інтегрує моніторинг IT та OT середовищ із використанням хмарного SIEM Google SecOps та аналітичної платформи Elastic, що забезпечує централізований збір журналів подій, виявлення підозрілих патернів та автоматичне сповіщення про загрози [12].

4. SOC-центр аеропорту Manchester Airports Group (Велика Британія) в якому функція моніторингу реалізовувалися через аутсорсингову модель з власною аналітичною командою та технологічною платформою на основі Microsoft Sentinel і Microsoft Defender XDR. Застосовано пілотну гібридну модель SOC-центру. Здійснюється централізована обробка інцидентів з різних джерел та підвищена ефективність моніторингу за рахунок зростання обробки подій з 5 000 до 80 000 за секунду, а охоплення активів – з 70% до 95% [13,14].

5. Інтегрований центри безпеки в Terminal 4 John F. Аеропорту Kennedy International Airport (США), який об'єднує SOC, AOCC та системи управління фізичною безпекою. Така інтеграція забезпечує централізований збір і кореляцію даних із систем відеоспостереження, контролю доступу та операційних сервісів, а також координацію реагування на інциденти у взаємодії з правоохоронними органами [15].

6. Централізований ситуаційний SOC-центр управління подіями фізичної та операційної безпеки на базі платформи Innovative Security Manager аеропорту Copenhagen Airport. Система забезпечує безперервний моніторинг безпекової ситуації, реєстрацію подій, координацію дій та документування інцидентів [16].

Узагальнені організаційні моделі Security Operations Center у цивільній авіації показані в табл. 1.

Представлені організаційні моделі демонструють варіативність підходів до структуризації кібероперацийної функції у цивільній авіації, окрім цього їх об'єднує спільна функціональна спрямованість. Незалежно від рівня автономії або способу ресурсного забезпечення, всі моделі орієнтовані на централізацію моніторингу подій безпеки, забезпечення безперервного функціонування механізмів виявлення інцидентів та координацію реагування в межах критичної інфраструктури сертифікованого аеропорту. Практика провідних аеропортів демонструє щонайменше три стабільні організаційні конфігурації: внутрішній спеціалізований центр (in-house), керований SOC (managed) та гібридні підходи, які відображають перехід від аутсорсингу до власної операційної спроможності. Такий підхід цілком логічний для обґрунтування використання спеціалізованих SOC-центрів в складні суб'єктів авіаційної діяльності критичної інфраструктури авіаційної галузі України.

Концептуальні засади побудови Security Operations Center в системі кіберстійкості суб'єктів авіаційної діяльності України

Законом України «Про критичну інфраструктуру» №3931-IX редакція від 21.09.2024 визначено, що транспортна система віднесена до секторів критичної інфраструктури. Закон встановлює обов'язок забезпечення стійкості функціонування об'єктів критичної інфраструктури та впровадження заходів з управління ризиками, зокрема і кіберризиками [20]. Водночас Закон України «Про основні засади забезпечення кібербезпеки України» №2163-VIII визначає об'єкти критичної інфраструктури як пріоритетні для захисту та встановлює необхідність створення систем виявлення, реагування та усунення наслідків кіберінцидентів. Оператори критичної інфраструктури та власники об'єктів критичної інформаційної інфраструктури належать до суб'єктів забезпечення кібербезпеки. До їх повноважень віднесено здійснення заходів з виявлення та реагування на кіберінциденти, усунення їх наслідків та забезпечення інформаційного обміну щодо кіберзагроз. Нормативне підґрунтя участі таких суб'єктів у загальнодержавній системі реагування визначене та передбачає створення та функціонування національної системи реагування на кіберінциденти, кібератаки та кіберзагрози щодо об'єктів критичної інформаційної інфраструктури. Уповноваженим органом, що забезпечує функціонування цієї системи, є Державна служба спеціального зв'язку та захисту інформації України. До її складу входить CERT-UA як національна команда реагування, що здійснює моніторинг і аналіз даних про кіберінциденти, надає попередження та рекомендації з реагування, забезпечує інформаційний обмін та координацію дій у межах національної системи реагування.

Законодавством України сформовано систему реагування на кіберзагрози, згідно якого критична інфраструктура сертифікованих аеропортів не є ізольованою, а навпаки, виступає учасником національної системи кіберзахисту. Реалізація обов'язків мережі відповідних операторів передбачає наявність у суб'єкта критичної інфраструктури внутрішньої операційної спроможності до: безперервного виявлення кіберінцидентів;

їх документування та аналізу; оперативної ескалації інформації; забезпечення технічного обміну даними з CERT-UA; виконання рекомендацій щодо реагування.

Таблиця 1

Узагальнені організаційні моделі Security Operations Center у цивільній авіації

Модель SOC	Організаційна характеристика	Типові риси функціонування	Стратегічні особливості застосування
Внутрішній (In-house) SOC	Спеціалізований підрозділ, створений у структурі оператора авіаційної інфраструктури	Цілодобовий моніторинг; формування власної експертної команди; повний контроль над процесами виявлення та реагування	Забезпечення високого рівня автономності та конфіденційності; потреба значних кадрових і фінансових ресурсів
Керований (Managed) SOC	Операційні функції передаються зовнішньому провайдеру за договором сервісного обслуговування	Безперебійне спостереження; централізований моніторинг; можливе охоплення IT та OT середовищ	Можливість швидко розгорнути кібероперацію функцію; зменшення навантаження на внутрішній персонал; часткова залежність від зовнішнього постачальника
Гібридна модель SOC	Поєднання внутрішньої команди та зовнішньої підтримки	Поступове нарощування власної спроможності; масштабування зони покриття; розширення огляду подій	Перехідна модель або модель для великих груп операторів; забезпечення балансу між контролем і ресурсною ефективністю
Інтегрований Security Operations Center (широкий безпековий контур)	Централізований центр управління безпековими операціями з інтеграцією різних потоків даних	Оперативний огляд у реальному часі; координація інцидентів; інтеграція з системами фізичної та операційної безпеки; безперервний режим функціонування	Підвищення ситуаційної обізнаності на рівні всієї інфраструктури; поєднання кібер та фізичних аспектів безпеки

В інакшому випадку оператор не може виконувати встановлені законом функції, оскільки не забезпечується необхідна вимога постійного моніторингу подій інформаційної безпеки, кореляції журналів, аналізу індикаторів компрометації та централізованого управління інцидентами. Забезпечення технічного обміну даними з CERT-UA з максимальною ефективністю в межах специфіки функціонування та взаємодії всіх критичних субєктів авіаційної діяльності здатен реалізувати спеціалізований SOC-центр. Головна законодавча вимога - безперервна інтеграція до систем управління безпекою (моніторинг, аналіз, обмін інформацією, реагування та документація та взаємодії з CERT-UA) повністю виконується. Отже, необхідність створення спеціалізованих SOC-центрів в сертифікованих ICAO міжнародних аеропортах України має нормативно-правове обґрунтування та виступає організаційною формою реалізації покладених законом функцій з виявлення, реагування та інформаційної взаємодії в межах реагування на кіберінциденти [18-21].

Структурно спеціалізований SOC-центр аеропорту доцільно розглядати як централізований операційний підрозділ, інтегрований до системи управління безпекою та ризиками. Його функціонування охоплює як інформаційні системи (IT-сегмент), так і технологічні системи (OT-сегмент), що експлуатуються в межах інфраструктури аеропортів. Такий підхід відповідає сучасній практиці моніторингу критичної інфраструктури. Інформаційний сегмент охоплює корпоративні системи управління, мережеву інфраструктуру, серверні та хмарні ресурси, а також пасажирські сервіси. Ці системи забезпечують адміністративну та сервісну діяльність аеропорту і є обов'язковими об'єктами кіберзахисту. Технологічний сегмент на відміну від IT, безпосередньо пов'язаний із фізичними процесами та операційною діяльністю. До нього належать Оперативна база даних аеропорту (AODB), системи обробки багажу (BHS), диспетчерські комплекси, енергетична інфраструктура та системи фізичної безпеки. Функціональна модель SOC-центру повинна передбачати безперервний збір та аналіз подій з обох середовищ із подальшою кореляцією між ними. Важливо, що інцидент у IT-сегменті може мати наслідки для OT-систем, а отже - для операційної безпеки аеропортів. Саме тому оцінка інцидентів у моделі SOC повинна включати визначення їхнього потенційного впливу на безпеку польотів та безперервність аеропортових процесів.

Структурно-функціональна модель SOC-центру суб'єкта авіаційної діяльності показана на рис. 1.

Модель демонструє інтеграцію двох взаємопов'язаних доменів - інформаційних та технологічних систем, що експлуатуються в межах аеропорту. SOC у цій моделі виступає централізованим аналітичним та координаційним центром, що агрегує події з різнорідних середовищ та формує єдину кібербезпекову ситуації.

Особливістю моделі є орієнтація не лише на технічне виявлення загроз, а й на управлінський аспект - інтеграцію результатів реагування до процесів оцінки ризиків, коригування внутрішніх процедур та підвищення кіберстійкості. Таким чином, SOC розглядається як елемент циклічної системи безперервного вдосконалення.

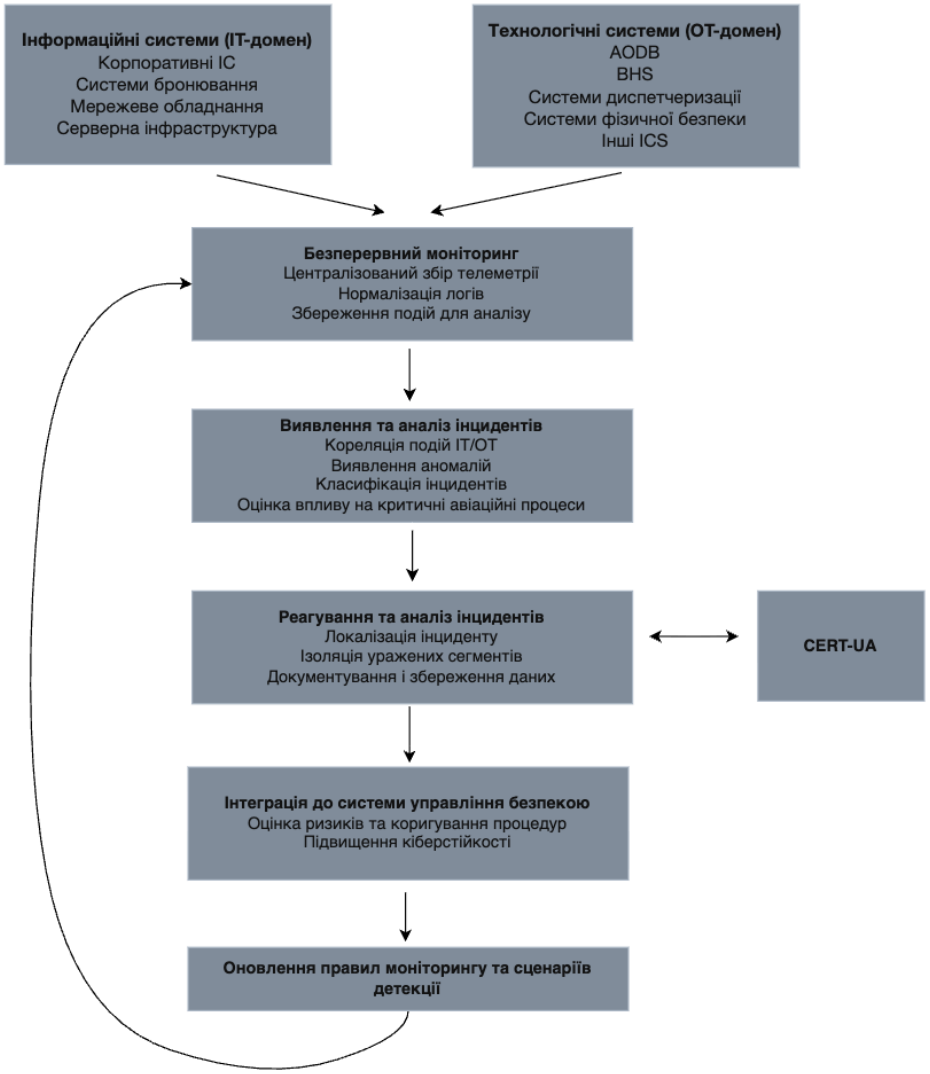

Рис. 1. Структурно-функціональна модель SOC-центру суб'єкта авіаційної діяльності

Також передбачено нормативно визначену взаємодію з національною системою реагування на кіберінциденти, зокрема з CERT-UA, що забезпечує обмін інформацією про загрози, індикатори компрометації та рекомендації щодо реагування. Отже, запропонована модель представляє комплексну, інтегровану та адаптивну систему, що поєднує технічний моніторинг, аналітичну обробку, операційне реагування та управлінське вдосконалення, забезпечуючи стійкість аеропортової інфраструктури до кіберзагроз у межах національної системи кібербезпеки.

Методологічні засади побудови та впровадження SOC суб'єкта авіаційної діяльності

Методологія побудови спеціалізованого SOC-центру суб'єкта авіаційної діяльності повинна розглядатися як формалізована послідовність організаційно-технологічних дій, спрямованих на формування операційної спроможності забезпечення кіберстійкості критичної авіаційної інфраструктури. Розробка методології полягає не лише у створенні технічної платформи моніторингу. Це системне інтегрування функцій виявлення, аналізу, реагування та управлінського вдосконалення у межах існуючої системи управління безпекою аеропорту. Методологічною основою виступає ризик-орієнтований підхід, відповідно до якого обсяг функціонування SOC визначається критичністю активів та потенційним впливом кіберінцидентів на безпеку польотів, безперервність операцій і захист інформації. Поетапний методологічний підхід побудови спеціалізованого SOC-центру суб'єкта авіаційної діяльності:

Етап №1. Початковий етап визначення операційного контуру спеціалізованого SOC-центру, що передбачає ідентифікацію інформаційних і технологічних систем, встановлення їх взаємозв'язків та класифікацію відповідно до рівня впливу на авіаційні процеси. Такий підхід забезпечує галузеву релевантність моделі та виключає формальне впровадження стандартних корпоративних рішень без урахування специфіки аеропортової інфраструктури.

Етап №2. Етап полягає у формуванні архітектури централізованого моніторингу, яка забезпечує безперебійне спостереження за подіями безпеки в IT та OT сегментах. На даному етапі відбувається формування єдиного аналітичного простору, в межах якого здійснюється агрегування, нормалізація та кореляція подій із різнорідних джерел. Інтеграція технологічних систем до контуру моніторингу є обов'язковою умовою, оскільки саме їх компрометація може призвести до порушення функціонування критичних авіаційних процесів.

Етап №3. Формування аналітичної спроможності спеціалізованого SOC-центру, що передбачає розроблення сценаріїв детекції, визначення критеріїв класифікації інцидентів та процедури оцінювання їх впливу на операційну діяльність аеропорту. Особливістю авіаційного середовища є необхідність поєднання технічного аналізу з оцінкою наслідків для безпеки польотів і обслуговування пасажирів, що вимагає міжфункціональної взаємодії між підрозділами.

Етап №4. Формалізація процедур реагування, які трансформують аналітичні висновки у керовані дії. Процедури повинні визначати алгоритми локалізації, порядок ізоляції уражених сегментів, механізми документування та умови взаємодії з національною системою реагування на кіберінциденти CERT-UA. Ключовою ознакою зрілості моделі є інтеграція SOC-центр до системи управління безпекою та ризиками, оскільки результати інцидентів повинні використовуватися для перегляду оцінки ризиків, удосконалення політик та коригування внутрішніх регламентів. У такий спосіб SOC-центр сприяє підвищенню кіберстійкості аеропорту.

Етап №5. Впровадження механізму безперервного вдосконалення, що передбачає післяінцидентний аналіз, оновлення правил моніторингу та періодичну перевірку готовності персоналу. Циклічність процесу забезпечує адаптивність до змін ландшафту загроз.

Авторами запропоновано узагальнене кортежне математичне представлення методологічного підходу реалізації спеціалізованого SOC-центру, що охоплює структуру суб'єктів авіаційної діяльності в межах функціонування міжнародного сертифікованого ICAO аеропорту України:

$$SOC_{airport} = \{\bigcup_{i=1}^{n} L_i\} = \{L_1, .L_2, L_3, \dots, L_n\} \quad (1)$$

де, $L_i \subseteq SOC_{airport}$, $i = 1, \dots, n$ - ключовий компонент кортежної моделі характеристик, що демонструє *i*-й шар розгортання архітектури SOC-центру, *n* – кількість шарів.

Наприклад, при $n = 5$, кортежна модель для узагальненої математичної моделі (1) буде виглядати наступним чином:

$$SOC_{airport} = \{\bigcup_{i=1}^{n} L_i\} = \{L_1, L_2, L_3, L_4, L_5\} = \{IL, ML, AL, RL, CL\} \quad (2)$$

де $L_1 = IL = "Infrastructure\ Layer"$ - шар архітектури SOC-центру, що визначає критичні складові інфраструктури аеропорту, які створюють, передають, зберігають та/або обробляють дані, що мають значення для авіаційної безпеки та операційної діяльності;

$L_2 = ML = "Monitoring\ Layer"$ - рівень моніторингу збирає телеметрію з інформаційно-комунікаційних систем аеропорту, перетворює фізичні та цифрові події у формалізовані дані;, формує базу для SIEM-аналізу, визначає первинні ознаки інцидентів.

$L_3 = AL = "Analytics\ Layer"$ - аналітичний рівень виконує інтелектуальне перетворення подій у кіберінциденти, забезпечуючи ситуаційну обізнаність SOC щодо стану кібербезпеки аеропорту. Цей рівень є центром прийняття аналітичних рішень.

$L_4 = RL = "Response\ Layer"$ - рівень реагування забезпечує локалізацію, нейтралізацію та мінімізацію наслідків кіберінцидентів шляхом автоматизованого та/або керованого реагування. Рівень трансформує аналітичні висновки у практичні дії.

$L_5 = CL = "Cryptographic\ Layer\ "$ - криптографічний рівень довіри забезпечує довіреність інформаційних потоків SOC**,** гарантуючи автентичність, конфіденційність та цілісність даних між усіма компонентами авіаційної інфраструктури.

Далі узагальнено розпишемо кожен з рівнів з врахуванням функціональної можливості спеціалізованого SOC-центру

1) $L_1 = IL = "Infrastructure\ Layer"$

$$IL = \{\bigcup_{j=1}^{m} IL_j\} = \{IL_1, IL_2, IL_3, \dots, IL_m\}, \quad (3)$$

де $IL_j \subseteq IL, (j = 1, \dots, m)$, j - критична складова інфраструктури аеропорту, m– їх кількість.

Наприклад при $m = 6$ формулу (3) можна представити як:

$IL = \{\bigcup_{j=1}^{m} ILj\} = \{IL_1, IL_2, IL_3, IL_4, IL_5, IL_6\} = \{IT, OT, CSN, Cloud, Meteo, Energo\}$, де

IT – інформаційні системи (AODB, Check-in), *OT* – операційні системи (BHS), *CNS* – авіаційні системи (ATC, ILS (GLS), *Cloud* - хмарні сервіси, *Meteo* – метерологічні системи аеропорту, *Energo* – енергетичні системи аеропорту.

2) $L_2 = ML = "Monitoring\ Layer"$

$$ML = \{\bigcup_{j=1}^{m} ML_j\} = \{ML_1, ML_2, ML_3, \dots, ML_m\}, \quad (4)$$

де $ML_j \subseteq ML, (j = 1, \dots, m)$, j - складова рівня моніторингу, m– їх кількість.

Наприклад при $m = 5$ формулу (4) можна представити як:

$ML = \{\bigcup_{j=1}^{m} ML_j\} = \{ML_1, ML_2, ML_3, ML_4, ML_5\} = \{N, F, S, D, E\}$, де

N – множина вузлів спостереження, *F* – інформаційні потоки, *S* – сенсори (системи IDS, OT sensors, NetFlow collectors), *D* – дані моніторингу, *E* – події безпеки.

3) $L_3 = AL = "Analytics\ Layer"$

$$AL = \{\bigcup_{j=1}^{m} AL_j\} = \{AL_1, AL_2, AL_3, \dots, AL_m\}, \quad (5)$$

де $AL_j \subseteq AL, (j = 1, \dots, m)$, j - складова аналітичного рівня, m– їх кількість.

Наприклад при $m = 5$ формулу (5) можна представити як:

$$AL = \{\bigcup_{j=1}^{m} AL_j\} = \{AL_1, AL_2, AL_3, AL_4\} = \{E, R, M, I, Risk\},$$

де E – множина подій, R – правила та алгоритми кореляції, M - аналітичні методи та моделі, I – правила та алгоритми формування інциденту, $Risk$ – методи та алгоритми розрахунку ризику

4) $L_4 = RL = "Response\ Layer"$

$$RL = \{\cup_{j=1}^{m} RL_j\} = \{RL_1, RL_2, RL_3, \ldots, RL_m\}, \quad (6)$$

де $RL_j \subseteq RL, (j = 1, \ldots, m)$, j - складова рівня реагування, m– їх кількість.

Наприклад при $m = 4$ формулу (6) можна представити як:

$$RL = \{\cup_{j=1}^{m} RL_j\} = \{RL_1, RL_2, RL_3, RL_4\} = \{I, H, P, T\}, \text{ де}$$

I – правила та алгоритми формування інциденту, H – Дії реагування на інцидент з подальшим блокуванням, ізолюванням чи відновленням системи, P – Incident Response Playbooks сценарії реагування на кіберінциденти, T – час реагування

5) $L_5 = CL = "Cryptographic\ Layer\ "$ -

$$CL = \{\cup_{j=1}^{m} CL_j\} = \{CL_1, CL_2, CL_3, \ldots, CL_m\} \quad (7)$$

де $CL_j \subseteq CL, (j = 1, \ldots, m)$, j - складова криптографічного рівня довіри, m– їх кількість.

Наприклад при $m = 5$ формулу (7) можна представити як:

$$CL = \{\cup_{j=1}^{m} CL_j\} = \{CL_1, CL_2, CL_3, CL_4\} = \{PKI, KMS, ALG, ENC, AUTH\}, \text{ де}$$

PKI – методи та моделі реалізації інфраструктури відкритих ключів, *KMS* – системи управління криптографічними ключами, *ALG* – криптографічні алгоритми, *ENC* – системи шифрування,*AUTH* – системи автентифікації.

Кожен рівень кортежної моделі SOC-центру аеропорту виконує окрему функціональну роль: інфраструктурний рівень формує інформаційне середовище, рівень моніторингу забезпечує спостережуваність, аналітичний рівень — інтерпретацію подій, рівень реагування — мінімізацію наслідків інцидентів, а криптографічний рівень — довіреність інформаційних потоків та суб'єктів взаємодії. Таким чином, розв'язано нову наукову задачу формалізації процесу забезпечення кіберзахисту інформаційних потоків об'єктів цивільної авіації шляхом побудови оптимізаційної математичної моделі спеціалізованого SOC-центру, яка інтегрує моніторинг, аналітику, реагування та криптографічний захист у єдину систему мінімізації ризику компрометації.

Висновки з даного дослідження
і перспективи подальшого розвитку у даному напрямку

Проведений аналіз підтвердив, що сучасні суб'єкти авіаційної діяності функціонує як складна інтегрована система, яка поєднує інформаційні та технологічні компоненти, а отже потребує централізованого та безперервного механізму контролю кіберризиків. Дослідження світової практики функціонування спеціалізованих SOC-центрів в міжнародних сертифікованих аеропортах продемонструвало, що ефективна модель передбачає цілодобовий моніторинг, інтеграцію різнорідних доменів, формалізовані процедури реагування та включення результатів інцидентів до процесів управління ризиками. Таким чином, спеціалізований SOC-центр розглядається не як допоміжний IT-підрозділ, а як операційний центр забезпечення стійкості критичних процесів. Без урахування міжнародних стандартів та рекомендованих практик (ICAO, ENISA, FAA, тощо) формування ефективної моделі спеціалізованих SOC-центрів для суб'єктів цивільної авіації України є неможливим, оскільки авіаційна галузь має глобальний характер та функціонує у межах уніфікованих вимог до безпеки. Відповідність цим вимогам визначає як технічні параметри системи моніторингу, так і організаційні механізми взаємодії. На основі узагальнення світового досвіду та національного нормативного контексту запропоновано структурно-функціональну модель спеціалізованого SOC-центру суб'єкта авіаційної діяльності, що відображає замкнений цикл безперервного моніторингу, виявлення, реагування, інтеграції до системи управління безпекою та постійного вдосконалення. Запропоновано методологію побудови та впровадження спеціалізованого SOC-центру, яка передбачає послідовне формування операційного контуру, архітектури моніторингу, аналітичної спроможності, процедур реагування, управлінської інтеграції та взаємодії з CERT-UA. Створення спеціалізованих SOC-центрів для аеропортів України є необхідною умовою підвищення кіберстійкості критичної авіаційної інфраструктури.

Література

1. Directive (EU) 2022/2555 (NIS2). Annex I - Sectors of high criticality. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

2. ENISA, Threat Landscape 2024. URL:https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

3. ENISA Threat Landscape 2025. URL:https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf

4. COMMISSION IMPLEMENTING REGULATION (EU) 2023/203. URL: https://eur-lex.europa.eu/eli/reg_impl/2023/203/oj/eng

5. NIST Special Publication 800-53 Revision 5 «Security and Privacy Controls for Information Systems and Organizations». URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

6. Poloato Security Operations Center (SOC) Roles and Responsibilities. URL: https://www.paloaltonetworks.com/cyberpedia/soc-roles-and-responsibilities

7. Reeves, A., & Ashenden, D. (2023). Understanding decision making in security operations centres: building the

case for cyber deception technology. Frontiers in psychology, 14, 1165705. URL: https://doi.org/10.3389/fpsyg.2023.1165705
8. IBM What is cyber resilience? URL: https://www.ibm.com/think/topics/cyber-resilience
9. Identify, Protect, Detect, Respond and Recover: The NIST Cybersecurity Framework. URL: https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework
10. Australia – Sydney Airport Gets 24/7 Security Operations Center. URL: https://eaasp.org/australia-sydney-airport-gets-24-7-security-operations-center/
11. Prague Airport Enhances Cyberattack Protection with New Cyber Security Operational Center. URL: https://www.aviationpros.com/airport-business/airport-infrastructure-operations/press-release/21156748/prague-airport-prague-airport-enhances-cyberattack-protection-with-new-cyber-security-operational-center
12. Flughafen Stuttgart – Round-the-clock cyber defence: Stuttgart Airport relies on Managed SOC. URL: https://www.bechtle.com/de-en/about-bechtle/references/stuttgart-airport
13. MAG transforms security operations centre to improve cyber resilience. URL: https://www.britishaviationgroup.co.uk/knowledge/mag-transforms-security-operations-centre-to-improve-cyber-resilience/
14. Manchester Airport Group Increases Security Event Visibility by 1500%. URL: https://www.bridewell.com/insights/news/detail/manchester-airport-group-increases-security-event-visibility-by-1500-with-bridewell-consulting
15. JFK Airport's Terminal 4 Debuts Security Operations Center. URL: https://www.aviationpros.com/airport-business/airport-infrastructure-operations/press-release/12412592/jfk-international-air-terminal-llc-jfkiat-jfk-airports-terminal-4-debuts-security-operations-center
16. Security operations at Copenhagen airport to new heights. URL: https://www.innovative.dk/en/customers-cases/airport-case/
17. Resolutions adopted by the assembly ICAO. URL: https://www2023.icao.int/Meetings/A40/Documents/Resolutions/a40_res_prov_en.pdf
18. Commission delegated regulation (EU) 2022/1645. URL: https://eur-lex.europa.eu/eli/reg_del/2022/1645/oj
19. ENISA how to setup up CSIRT and SOC good practice guide. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20How%20to%20setup%20CSIRT%20and%20SOC.pdf
20. Закон України «Про критичну інфраструктуру». URL: №3931-IX https://zakon.rada.gov.ua/laws/show/1882-20#Text
21. Закон України «Про основні засади забезпечення кібербезпеки України» №2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

References

1. Directive (EU) 2022/2555 (NIS2). Annex I - Sectors of high criticality. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
2. ENISA, Threat Landscape 2024. URL:https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf
3. ENISA Threat Landscape 2025. URL:https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf
4. COMMISSION IMPLEMENTING REGULATION (EU) 2023/203. URL: https://eur-lex.europa.eu/eli/reg_impl/2023/203/oj/eng
5. NIST Special Publication 800-53 Revision 5 «Security and Privacy Controls for Information Systems and Organizations». URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
6. Poloato Security Operations Center (SOC) Roles and Responsibilities. URL: https://www.paloaltonetworks.com/cyberpedia/soc-roles-and-responsibilities
7. Reeves, A., & Ashenden, D. (2023). Understanding decision making in security operations centres: building the case for cyber deception technology. Frontiers in psychology, 14, 1165705. URL: https://doi.org/10.3389/fpsyg.2023.1165705
8. IBM What is cyber resilience? URL: https://www.ibm.com/think/topics/cyber-resilience
9. Identify, Protect, Detect, Respond and Recover: The NIST Cybersecurity Framework. URL: https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework
10. Australia – Sydney Airport Gets 24/7 Security Operations Center. URL: https://eaasp.org/australia-sydney-airport-gets-24-7-security-operations-center/
11. Prague Airport Enhances Cyberattack Protection with New Cyber Security Operational Center. URL: https://www.aviationpros.com/airport-business/airport-infrastructure-operations/press-release/21156748/prague-airport-prague-airport-enhances-cyberattack-protection-with-new-cyber-security-operational-center
12. Flughafen Stuttgart – Round-the-clock cyber defence: Stuttgart Airport relies on Managed SOC. URL: https://www.bechtle.com/de-en/about-bechtle/references/stuttgart-airport
13. MAG transforms security operations centre to improve cyber resilience. URL: https://www.britishaviationgroup.co.uk/knowledge/mag-transforms-security-operations-centre-to-improve-cyber-resilience/
14. Manchester Airport Group Increases Security Event Visibility by 1500%. URL: https://www.bridewell.com/insights/news/detail/manchester-airport-group-increases-security-event-visibility-by-1500-with-bridewell-consulting
15. JFK Airport's Terminal 4 Debuts Security Operations Center. URL: https://www.aviationpros.com/airport-business/airport-infrastructure-operations/press-release/12412592/jfk-international-air-terminal-llc-jfkiat-jfk-airports-terminal-4-debuts-security-operations-center
16. Security operations at Copenhagen airport to new heights. URL: https://www.innovative.dk/en/customers-cases/airport-case/
17. Resolutions adopted by the assembly ICAO. URL: https://www2023.icao.int/Meetings/A40/Documents/Resolutions/a40_res_prov_en.pdf
18. Commission delegated regulation (EU) 2022/1645. URL: https://eur-lex.europa.eu/eli/reg_del/2022/1645/oj
19. ENISA how to setup up CSIRT and SOC good practice guide. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20How%20to%20setup%20CSIRT%20and%20SOC.pdf
20. Law of Ukraine «On Critical Infrastructure». URL: №3931-IX https://zakon.rada.gov.ua/laws/show/1882-20#Text
21. Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine» №2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text