

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

ДРАГУНЦОВ РОМАН ІГОРОВИЧ

УДК 004.056.5:004.75

ДИСЕРТАЦІЯ
МЕТОДИ ЗБОРУ, ОБРОБКИ ТА АНАЛІЗУ ІНФОРМАЦІЇ В
КОМП'ЮТЕРНИХ СИСТЕМАХ УПРАВЛІННЯ ПОДІЯМИ БЕЗПЕКИ В
УМОВАХ ОБМЕЖЕНОЇ СПОСТЕРЕЖНОСТІ

122 Комп'ютерні науки

12 Інформаційні технології

Подається на здобуття наукового ступеня доктор філософії

Дисертація містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Р.І. Драгунцов

Науковий керівник: Зубок Віталій Юрійович, доктор технічних наук, старший
дослідник

Київ — 2026

АНОТАЦІЯ

Драгунцов Р.І. Методи збору, обробки та аналізу інформації в комп'ютерних системах управління подіями безпеки в умовах обмеженої спостережності.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки. – Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, 2026

У дисертації розв'язано науково-прикладну задачу підвищення спостережності інформаційних систем у процесах моніторингу та реагування на інциденти кібербезпеки за умов обмеженої спостережності, спричиненої воєнними впливами і деградацією інфраструктури, зокрема масовими відключеннями електропостачання та зв'язку. Розроблено методологічний апарат формалізації «втрати спостережності» як вимірюваної властивості активу; запропоновано методи атрибутивного профілювання активів і контролю на основі метрик, що враховують динамічність складу інфраструктури, резервування, географічну приналежність і контекст загроз; сформовано високорівневі вимоги та прототипну архітектуру технічного рішення, орієнтованого на інтеграцію з існуючими системами обробки, аналізу та реагування на події безпеки з урахуванням критерію агностичності до технологічної платформи.

Метою роботи є підвищення ефективності процесів збору та аналізу інформації в комп'ютерних системах управління подіями безпеки шляхом удосконалення процесів збору та аналізу інформації в умовах деградації інфраструктури інформаційно-комунікаційних систем.

Об'єктом дослідження є процеси збору, аналізу інформації про події та інциденти, а також процеси прийняття рішень в операційних центрах кіберзахисту, що включають збір і кореляцію телеметрії, виявлення аномалій та ініціювання реакцій у розподілених інформаційних системах із частковою втратою керування, які зазнають деградації доступності та спостережності

внаслідок зовнішніх впливів, зокрема порушень електроживлення та каналів зв'язку.

Предметом дослідження є методи збору та аналізу інформації в операційних центрах кіберзахисту спрямовані на підвищення спостережності інформаційних систем.

Вперше розроблено формалізовану постановку задачі підвищення спостережності інформації у контексті деградації інфраструктури, у якій «втрата спостережності» визначається як стан системи, за якого зменшується повнота та/або достовірність телеметрії до рівня, що порушує коректність виконання щонайменше одного класу процедур операційного центру кіберзахисту (виявлення, розслідування, атрибуція, реагування), а перехід у такий стан описується вимірюваними ознаками доступності джерел подій і узгодженості інвентарних даних;

Дістав подальшого розвитку метод атрибутивного профілювання активів для потреб операційних центрів кіберзахисту, у якому для кожного активу формується вектор атрибутів, релевантних для оцінювання спостережності та ризиків інтерпретації телеметрії за умов деградації інфраструктури;

Виконано проектування архітектури прототипу технічного рішення підвищення спостережності, в якій виділено контури: інвентаризації та злиття даних про активи, аналітики подій/інцидентів, активного реагування, атрибутивного профілювання та обчислення правил/метрик, а також візуалізації та звітності.

Розроблено методологію, орієнтовану на корекцію процесів обробки сигналів в операційних центрах кіберзахисту, спрямовану на виявлення та врахування деградації спостережності, як необхідної умови коректної інтерпретації сигналів про кіберзагрози за умов воєнних впливів;

У роботі виконано аналіз умов функціонування операційних центрів кіберзахисту у середовищі з деградацією інфраструктури та неповнотою телеметрії; встановлено класи операційних помилок, що виникають при

змішуванні технічної недоступності компонентів і можливих зловмисних впливів; визначено вимоги до даних і процедур, які забезпечують коректність інтерпретації подій у таких умовах. Побудовано методологію оцінювання спостережності та корекції процесів обробки сигналів, що включає метрики втрати спостережності як окремий контур пріоритезації дій та обрання реакцій. Проаналізовано архітектурні підходи до реалізації запропонованих методів у складі типових технологічних компонентів систем обробки подій безпеки та обґрунтовано доцільність відкритої модульної архітектури. Сформовано верхньорівневі вимоги до прототипу, розроблено склад і функції ключових модулів, визначено логіку обміну даними між ними та принципи оркестрації обчислень атрибутів і метрик. Запропоновані рішення орієнтовані на підвищення відтворюваності операційних висновків, зниження ризику некоректної атрибуції стану активів у періоди деградації та зменшення негативних впливів погіршеної спостережності військового часу на показники операційної роботи операційних центрів кіберзахисту.

Розділ 1 присвячено аналізу впливу сучасних умов функціонування інформаційно-комунікаційних систем на спостережність інформації в комп'ютерних системах управління подіями безпеки. У розділі систематизовано ключові фактори військового часу, що порушують повноту, своєчасність і достовірність телеметрії: деградацію енергетичної та телекомунікаційної інфраструктури, окупацію і фізичну втрату ІТ-активів, кадрову кризу, інтенсифікацію кібервійни, розрізненість нормативної бази та вимушену зміну архітектури ІКС. Визначено характер впливу цих факторів на процеси виявлення, аналізу та реагування, а також оцінено наявні підходи до протидії втраті спостережності, зокрема резервування електроживлення і каналів зв'язку, географічне розподілення інфраструктури та використання хмарних ресурсів.

Розділ 2 присвячено розробці методологічного апарату підвищення спостережності інформації в умовах деградації інфраструктури. У розділі побудовано дескриптивну модель впливу деградації електроживлення, каналів зв'язку, джерел телеметрії та інвентаризаційного контексту на якість операційної діяльності в комп'ютерних системах управління подіями безпеки.

Запропоновано підхід до атрибутивного профілювання активів і злиття інвентарних даних, визначено правила та метрики оцінювання втрати спостережності, введено атрибути динамізму активу і дескриптора загроз, а також сформовано принципи побудови контролів, що дозволяють відрізняти технічну деградацію від потенційної активності агента загроз.

Розділ 3 присвячено розробці вимог, архітектури та прототипу технічного рішення, що реалізує методи підвищення спостережності, запропоновані в розділі 2. У розділі сформовано проєкт відкритої модульної архітектури, до складу якої входять підсистема збору й аналізу подій на основі Security Information and Event Management (SIEM), підсистема активного реагування, підсистема інвентаризації та злиття даних, модулі обчислення динамізму й дескриптора загроз, підсистема контролів, а також підсистема візуалізації та звітності. Визначено вимоги до інтеграції, даних і синтетичних подій, а також сформовано склад експериментального стенду для перевірки ефективності запропонованих методів.

Розділ 4 присвячено експериментальній перевірці ефективності розроблених методів у комп'ютерній системі покращення спостережності. У розділі виконано порівняння базового режиму обробки подій і режиму із застосуванням запропонованої методології на сценаріях масової втрати електроживлення, деградації каналів зв'язку, відновлення після деградації та накладання зловмисної активності на тлі технічної недоступності. Отримані результати підтвердили зменшення кількості хибних інтерпретацій, підвищення точності класифікації, зниження операційного шуму та покращення пріоритезації подій за умов обмеженої спостережності.

Актуальність тематики визначається тим, що сучасні процеси обробки, аналізу та реагування на події та інциденти безпеки критично залежать від безперервного збору телеметрії та стабільності інфраструктурних компонентів, тоді як у воєнних умовах та при масових порушеннях енергоживлення/зв'язку спостерігається систематичне зниження доступності джерел журналювання, деградація каналів доставлення подій і прискорення динаміки змін

інфраструктури на тлі інтенсифікації активності агентів загроз. Традиційні засоби кореляції та реагування в даних умовах мають схильність до генерації некоректних висновків через змішування технічної недоступності й зловмисних впливів та втрату контексту щодо складу й стану активів.

Актуальність пов'язана з практичною потребою формалізувати «якість спостережності» як вимірювану величину. Без вимірюваних метрик втрати спостережності операційний центр кіберзахисту має обмежені можливості для об'єктивного обмеження достовірності аналітичних висновків і не може коректно пріоритезувати розслідування. Запропонований у роботі підхід забезпечує методологічну основу для постійного визначення стану спостережності та застосування даної оцінки в операційній роботі.

Практична значимість полягає у можливості безпосереднього впровадження запропонованих методів у процеси операційних центрів кібербезпеки з використанням запропонованої архітектури: модулі інвентаризації та злиття даних про активи, атрибутивного профілювання та обчислення контролів/метрик забезпечують можливість інтеграції з наявними компонентами технологічних платформ обробки та аналізу подій безпеки.

Ключові слова: спостережність, інформаційно-комунікаційна інфраструктура, моніторинг подій безпеки, система управління подіями інформаційної безпеки, реагування на інциденти, операційний центр кіберзахисту (SOC), руйнування критичної інфраструктури, обробка подій безпеки, виявлення кібератак, моніторинг інфраструктури, кібербезпека

SUMMARY

Drahuntsov R.I. Methods for the Collection, Processing, and Analysis of Information in Computer Systems for Security Event Management under Conditions of Limited Observability.

Dissertation for the degree of Doctor of Philosophy in Specialty 122 – Computer Science. – G.E. Pukhov Institute for Modelling in Energy Engineering of the National Academy of Sciences of Ukraine, Kyiv, 2026.

The dissertation solves an applied scientific problem of improving the observability of information systems in the processes of cybersecurity monitoring and incident response under conditions of limited observability caused by wartime impacts and infrastructure degradation, in particular large-scale disruptions of power supply and communication. A methodological apparatus is developed for formalizing “observability loss” as a measurable property of an asset. Methods of asset attribute profiling and control based on metrics are proposed, taking into account the dynamicity of infrastructure composition, redundancy, geographical affiliation, and threat context. High-level requirements and a prototype architecture of a technical solution are formulated, oriented toward integration with existing systems for the processing, analysis, and response to security events, while considering the criterion of technological platform agnosticism.

The aim of the dissertation is to improve the efficiency of information collection and analysis processes in computer systems for security event management by enhancing the processes of information collection and analysis under conditions of degradation of information and communication systems infrastructure.

The object of the research is the processes of collecting and analyzing information on events and incidents, as well as decision-making processes in cybersecurity operations centers. These processes include telemetry collection and correlation, anomaly detection, and response initiation in distributed information systems with partial loss of control, which undergo degradation of availability and

observability due to external impacts, in particular disruptions of power supply and communication channels.

The subject of the research is the methods of information collection and analysis in cybersecurity operations centers aimed at improving the observability of information systems.

For the first time, a formalized problem statement for improving information observability in the context of infrastructure degradation has been developed. In this statement, “observability loss” is defined as a system state in which the completeness and/or reliability of telemetry decreases to a level that disrupts the correct execution of at least one class of cybersecurity operations center procedures: detection, investigation, attribution, or response. The transition to such a state is described by measurable indicators of event source availability and consistency of inventory data.

The method of asset attribute profiling for the needs of cybersecurity operations centers has been further developed. In this method, an attribute vector is formed for each asset; the vector contains attributes relevant to assessing observability and the risks of telemetry interpretation under conditions of infrastructure degradation.

The architecture of a prototype technical solution for improving observability has been designed. The architecture distinguishes the following functional circuits: asset inventory and data fusion, event and incident analytics, active response, attribute profiling and computation of rules and metrics, as well as visualization and reporting.

A methodology has been developed that is oriented toward the correction of signal processing procedures in cybersecurity operations centers. The methodology is aimed at detecting and accounting for observability degradation as a necessary condition for the correct interpretation of cyber threat signals under wartime impacts.

The dissertation analyzes the operating conditions of cybersecurity operations centers in environments characterized by infrastructure degradation and incomplete telemetry. Classes of operational errors that arise when technical unavailability of components is conflated with possible malicious impacts are identified. Data and

procedure requirements necessary to ensure correct event interpretation under such conditions are defined. A methodology for assessing observability and correcting signal processing procedures is constructed; it includes observability loss metrics as a separate circuit for action prioritization and response selection. Architectural approaches to implementing the proposed methods within typical technological components of security event processing systems are analyzed, and the feasibility of an open modular architecture is substantiated. High-level requirements for the prototype are formulated, the composition and functions of key modules are developed, and the logic of data exchange between them and principles of orchestrating attribute and metric computations are defined. The proposed solutions are oriented toward increasing the reproducibility of operational conclusions, reducing the risk of incorrect attribution of asset states during degradation periods, and mitigating the negative impact of reduced wartime observability on the operational performance indicators of cybersecurity operations centers.

Chapter 1 is devoted to analyzing the impact of contemporary operating conditions of information and communication systems on information observability in computer systems for security event management. The chapter systematizes key wartime factors that disrupt the completeness, timeliness, and reliability of telemetry: degradation of energy and telecommunications infrastructure, occupation and physical loss of information technology assets, workforce crisis, intensification of cyberwarfare, fragmentation of the regulatory framework, and forced changes in the architecture of information and communication systems. The nature of the influence of these factors on detection, analysis, and response processes is determined. Existing approaches to counteracting observability loss are also evaluated, including power supply and communication channel redundancy, geographical distribution of infrastructure, and the use of cloud resources.

Chapter 2 is devoted to the development of a methodological apparatus for improving information observability under conditions of infrastructure degradation. The chapter constructs an analytical model of the influence of degradation of power supply, communication channels, telemetry sources, and inventory context on the

quality of operational activity in computer systems for security event management. An approach to asset attribute profiling and inventory data fusion is proposed. Rules and metrics for assessing observability loss are defined. The attributes of asset dynamicity and threat descriptor are introduced. Principles are also formulated for constructing controls that make it possible to distinguish technical degradation from potential activity of a threat agent.

Chapter 3 is devoted to the development of requirements, architecture, and a prototype of the technical solution that implements the observability improvement methods proposed in Chapter 2. The chapter formulates the design of an open modular architecture comprising the following components: an event collection and analysis subsystem based on Security Information and Event Management (SIEM); an active response subsystem; an inventory and data fusion subsystem; modules for computing dynamicity and the threat descriptor; a controls subsystem; and a visualization and reporting subsystem. Requirements for integration, data, and synthetic events are defined. The composition of an experimental testbed for evaluating the effectiveness of the proposed methods is also formulated.

Chapter 4 is devoted to experimental verification of the effectiveness of the developed methods in a computer system for improving observability. The chapter compares the baseline event processing mode with the mode using the proposed methodology across scenarios of large-scale power loss, communication channel degradation, recovery after degradation, and the superposition of malicious activity against a background of technical unavailability. The obtained results confirmed a reduction in the number of false interpretations, an increase in classification accuracy, a decrease in operational noise, and improved prioritization of events under conditions of limited observability.

The relevance of the topic is determined by the fact that modern processes of processing, analyzing, and responding to security events and incidents critically depend on continuous telemetry collection and the stability of infrastructure components. At the same time, under wartime conditions and during large-scale disruptions of power supply and communication, there is a systematic decrease in the

availability of logging sources, degradation of event delivery channels, and acceleration of infrastructure change dynamics against the background of intensified threat agent activity. This creates a situation in which traditional correlation and response tools may generate incorrect conclusions due to the conflation of technical unavailability and malicious impacts, as well as due to the loss of context regarding the composition and state of assets.

Additional relevance is associated with the practical need to formalize the “quality of observations” as a controllable quantity. Without measurable metrics of “observability loss,” a cybersecurity operations center has no basis for objectively limiting the reliability of analytical conclusions and cannot correctly prioritize investigations under conditions of telemetry deficit. The approach proposed in the dissertation provides an instrumental basis for such formalized control through the integration of asset inventory, attribute profiling, and observability controls.

The practical significance of the dissertation lies in the possibility of direct implementation of the proposed methods in cybersecurity operations center processes using the proposed architecture. The modules for asset inventory and data fusion, attribute profiling, and computation of controls and metrics provide the possibility of integration with existing components of technological platforms for security event processing and analysis.

Key words: observability, information and communication infrastructure, security event monitoring, Security Information and Event Management system, incident response, Security Operations Center, critical infrastructure destruction, cyberattack detection, security event correlation, infrastructure monitoring, cybersecurity

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у наукових періодичних виданнях інших держав із напрямку, з якого підготовлено дисертацію

[1] R. Drahuntsov, A. Symonov, O. Potenko, O. Dybach, and V. Zubok, “Cybersecurity monitoring during power outages: Use cases for enhanced infrastructure observability and potential implications for NPP combined events,” *Nuclear and Radiation Safety*, no. 3(107), pp. 17–29, 2025, doi: 10.32918/nrs.2025.3(107).02.

Внесок здобувача: збір та аналіз референсних даних, аналіз ключових проблем спостережності інформації в заданих умовах та референсних інфраструктурах, розробка методів та контролів виявлення порушення спостережності та усунення невизначеності в умовах деградації інфраструктури.

Статті у наукових виданнях, включених до Переліку наукових фахових видань України

[2] R. Drahuntsov and V. Zubok, “Modeling of cyber threats related to massive power outages and potential countermeasures,” *Elektronnoe Modelirovanie*, vol. 45, no. 3, pp. 116–128, 2023, doi: 10.15407/emodel.45.03.116.

Внесок здобувача: аналіз загроз та ризиків для ІКС, пов’язаних з атаками на енергосистему, порівняльний аналіз контрзаходів з енергетичної безпеки ІКС, формування пропозицій підходів до моделювання загроз з урахуванням факторів масштабних відключень електропостачання.

[3] R. Drahuntsov and V. Zubok, “Dynamic infrastructure components and system visibility during cybersecurity incident response,” *Cybersecurity: Education, Science, Technique*, no. 1(29), pp. 493–507, 2025, doi: 10.28925/2663-4023.2025.29.891.

Внесок здобувача: Ідентифікація аспектів видимості динамічних структур – визначення ключових прикладів динамічних інфраструктурних компонентів,

аналіз характеру впливу деградації енергетичної інфраструктури на динамічні компоненти ІКС.

[4] O. Popov and R. Drahuntsov, “Ключові виклики для операційних центрів кібербезпеки в умовах повномасштабної війни,” *Information Technology and Society*, no. 3(18), 2025, doi: 10.32689/maup.it.2025.3.19.

Внесок здобувача: збір статистичних даних, визначення ключових специфічних факторів впливу військового часу на процеси обробки інформації в операційних центрах кібербезпеки, аналіз впливів руйнування енергетичної та телекомунікаційної інфраструктури, окупації та втрати об’єктів ІТ інфраструктури, кібервійни на показники роботи операційних центрів кібербезпеки.

[5] R. Drahuntsov and V. Zubok, “Methods for maintaining the observability of information and communication infrastructure in conditions of full-scale war,” *Elektronnoe Modelirovanie*, vol. 48, no. 1, pp. 72–86, 2026, doi: 10.15407/emodel.48.01.072.

Внесок здобувача: дослідження наявних підходів до вирішення проблеми погіршення спостережності інформації, формування дескриптивної моделі впливів військового часу на операційні процеси обробки подій безпеки та функціонування операційних центрів кіберзахисту, розробка принципу зменшення невизначеності в розрізі спостережності інфраструктури, введення метрики «динамізм» інфраструктурного об’єкту, розробка атрибута «дескриптор загроз» для об’єктів ІКС.

Наукові праці, що засвідчують апробацію результатів наукової роботи

[6] R. Drahuntsov and V. Zubok, “A method for reducing the uncertainty caused by a power outage during a cyber incident response,” in *CEUR Workshop Proc.*, vol. 3887, pp. 226–236, 2024. [Online]. Available: ceur-ws.org/Vol-3887/paper20.pdf. Accessed: Feb. 24, 2026.

Внесок здобувача: Визначення ключових факторів впливу деградації енергетичної та комунікаційної інфраструктури на процес реагування на інциденти кіберзахисту; визначення класів операційних помилок, що виникають в процесах обробки подій безпеки в середовищі з деградацією телекомунікаційної та енергетичної інфраструктури; розробка алгоритму спрощення представлення ІКС під час реагування на інциденти кіберзахисту.

[7] V. Yu. Zubok and R. S. Drahuntsov, “Проекція принципів національної системи стійкості та резильєнтності критичної інформаційної інфраструктури,” in *Proc. Sci.-Pract. Conf. “Резильєнтність критичної інфраструктури – 2023”*, Kyiv, Ukraine, Jun. 21, 2023, pp. 104–108. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2023/06/Матеріали-конференції-Critical-Infrastructure-Resilience---2023.pdf. Accessed: Feb. 24, 2026.

Внесок здобувача: дослідження існуючої нормативної бази в розрізі кіберстійкості критичної інфраструктури.

[8] V. Yu. Zubok and R. S. Drahuntsov, “Особливості розслідування та реагування на інциденти кібербезпеки в умовах масових відключень електропостачання,” in *Proc. V Sci.-Pract. Conf. “Безпека енергетики в епоху цифрової трансформації” (БЕЕЦТ-2023)*, Kyiv, Ukraine, 2023, pp. 38–42. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2023/11/Матеріали-конференції-БЕЕЦТ-2023.pdf. Accessed: Feb. 24, 2026.

Внесок здобувача: дослідження підходів до обробки сигналів про інциденти в системах обробки та аналізу подій безпеки; оцінка впливу деградації інфраструктури на процеси реагування на інциденти кіберзахисту.

[9] R. Drahuntsov and V. Zubok, “Особливості атак з використанням соціального графу та підходи до захисту,” in *Proc. 2nd All-Ukrainian Sci.-Pract. Conf. “Theoretical and Applied Cybersecurity” (TACS-2024)*, Kyiv, Ukraine, 2024. [Online]. Available: is.ipt.kpi.ua/pdf/T24.pdf. Accessed: Feb. 24, 2026.

Внесок здобувача: збір статистичних даних про кібератаки з використанням соціальної інженерії; ідентифікація графового підходу до

формування ланцюжку атаки; ідентифікація ризиків пов'язаних з непрямыми атаками соціальної інженерії.

[10] V. V. Zubok, R. S. Drahuntsov, and V. Yu. Zubok, “Резильєнтність ERP-систем в умовах енергетичної кризи,” in *Proc. Sci.-Pract. Conf. “Кібербезпека енергетики”*, Kyiv, Ukraine, 2024, pp. 13–16. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2024/06/Матеріали-КБЕ-2024.pdf. Accessed: Feb. 24, 2026.

Внесок здобувача: оцінка впливу деградації енергетичної інфраструктури на спостережність ERP-систем.

[11] R. I. Drahuntsov, “Особливості інцидентів інформаційної безпеки з залученням шкідливого ПЗ в умовах кібервійни – аналіз та реагування,” in *Proc. Conf. Materials (v.2)*, Kyiv, Ukraine, 2024, pp. 65–68. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2024/05/Матеріали-конференції-2024-v-2.pdf. Accessed: Feb. 24, 2026.

[12] R. I. Drahuntsov and V. Yu. Zubok, “Проблематика інтеграції джерел виявлення технічних вразливостей в розрізі підтримки кіберстійкості критичної інфраструктури,” in *Proc. XLIII Sci.-Tech. Conf. Young Scientists and Specialists (PIMEE NAS of Ukraine)*, Kyiv, Ukraine, May 14, 2025, pp. 29–31. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2025/05/Materialy-KMV-2025.pdf. Accessed: Feb. 24, 2026.

Внесок здобувача: збір статистичної інформації про використання засобів управління вразливостями; формування переліку ключових проблем інтеграції джерел виявлення технічних вразливостей; формування математичної моделі проблематики процесу збільшення складності процесу управління вразливостями.

[13] R. I. Drahuntsov, “Алгоритм управління ризиками кібербезпеки в умовах знищення енергетичної інфраструктури,” in *Proc. Sci.-Pract. Conf. “Кібербезпека енергетики” (КБЕ-2025)*, Kyiv, Ukraine, 2025. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2025/05/Матеріали-КБЕ-2025-1.pdf. Accessed: Feb. 24, 2026.

[14] R. I. Drahuntsov, “Процедури threat hunting в сучасному SOC – ключові підходи та проблематика оцінки покриття,” in *Proc. Conf. “Цифрова трансформація кібербезпеки”*, pp. 40–42, 2025. [Online]. Available: duikt.edu.ua/uploads/p_2779_36484696.pdf. Accessed: Feb. 24, 2026.

[15] R. I. Drahuntsov and V. Yu. Zubok, “Застосування великих мовних моделей для автоматичної ідентифікації окремих атрибутів поверхні атаки активів в кібербезпеці,” in *Proc. Sci.-Pract. Conf. “ШІБ-2025”*. [Online]. Available: ipme.kiev.ua/konferencii/naukovo-praktichna-konferenciya-sib-2025/. Accessed: Feb. 24, 2026.

Внесок здобувача: розробка концепції застосування LLM для визначення дескриптора загроз активу; оцінка можливостей інтеграції LLM в процес управління активами.

Інші праці здобувача

[16] R. Drahuntsov and D. Rabchun, “Potential disguising attack vectors on security operations centers and SIEM systems,” *Cybersecurity: Education, Science, Technique*, no. 2(14), pp. 6–14, 2021, doi: 10.28925/2663-4023.2021.14.614.

Внесок здобувача: дослідження принципу розподілу сигналів для реагування в операційних центрах кіберзахисту; дослідження впливу операційного шуму на операційні процеси центрів кіберзахисту; формування гіпотези про можливості виконання відволікаючих атак на кібернетичну інфраструктуру, перевантаження та зміщення фокусу уваги аналітиків.

[17] R. Drahuntsov, D. Rabchun, and Z. Brzhevska, “Architecture security principles of the Android operating system,” *Cybersecurity: Education, Science, Technique*, no. 2(8), pp. 49–60, 2020, doi: 10.28925/2663-4023.2020.8.4960.

Внесок здобувача: дослідження існуючих архітектурних принципів операційних систем Android, ключових методів захисту та атак на дані системи.

ЗМІСТ

Анотація	2
SUMMARY.....	7
СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА.....	12
ЗМІСТ	17
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	23
ВСТУП.....	25
РОЗДІЛ 1. Аналіз впливу сучасних умов функціонування ІКС на спостережність інформації. Огляд існуючих методів та алгоритмів протидії.	32
1.1. Огляд існуючих методів обробки та аналізу інформації в комп'ютерних системах управління подіями безпеки	32
1.1.1. Збір та попередня обробка телеметрії.....	32
1.1.2. Детерміновані методи виявлення	34
1.1.3. Методи комплексної обробки подій	35
1.1.4. Методи агрегації та кореляції оповіщень	36
1.1.5. Кластеризація та аналіз першопричин.....	37
1.1.6. Статистичні методи та виявлення аномалій	38
1.1.7. Причинно-наслідні та графові методи	39
1.1.8. Методи контекстного збагачення.....	39
1.1.9. Методи ретроспективного аналізу та реконструкції інциденту	40
1.2. Огляд специфічних впливів на спостережність інформації в системах управління подіями безпеки в умовах повномасштабної війни	41
1.2.1. Руйнування енергетичної та телекомунікаційної інфраструктури ..	41
1.2.2. Окупація та втрата об'єктів ІТ-інфраструктури.....	42
1.2.3. Кадрова криза	43

1.2.4. Фактор кібервійни	44
1.3. Аналіз загроз та ризиків для ІКС, пов'язаних з атаками на енергосистему	44
1.3.1. Недоступність та простій бізнес-сервісів та додатків, відключення обладнання та систем.....	45
1.3.2. Необхідність додаткових витрат ресурсів команд підтримки та безпеки.....	45
1.3.3. Відключення контролів безпеки	45
1.3.4. Погіршення спостережності внаслідок перерв у постачанні журналів.	46
1.4. Оцінка впливу на спостережність інформації для кожного типу волатильних об'єктів.....	50
1.5. Технології та методи протидії впливам деградації інфраструктури на спостережність інформації.....	53
1.5.1. Резервування каналів зв'язку	54
1.5.2. Резервування електроживлення.	54
1.5.4. Географічне розподілення ІКС.....	55
1.5.5. Розподілення ІКС з використанням потужностей хмарних провайдерів.	55
1.6. Порівняльний аналіз технологій та методів протидії впливам відключень електропостачання	56
1.7. Оцінка ефективності існуючих підходів до протидії втраті спостережності в умовах деградації інфраструктури.....	57
1.7.1. Обмеження інфраструктурних методів підтримки спостережності	57
1.7.2. Вплив втрати спостережності на збір і попередню обробку телеметрії	60
1.7.3. Вплив на детерміновані методи виявлення	61
1.7.4. Вплив на комплексну обробку та кореляцію подій	62

1.7.5. Вплив на кластеризацію, статистичний і поведінковий аналіз	63
1.7.6. Вплив на причинно-наслідні та графові методи	63
1.7.7. Вплив на контекстне збагачення, оцінювання ризику та ретроспективний аналіз	64
1.7.8. Невирішені аспекти протидії втраті спостережності	65
Висновки	66
РОЗДІЛ 2. Розробка методів та алгоритмів покращення спостережності інформації.....	69
2.1. Визначення метрик оцінки впливу втрати спостережності та специфічних військових факторів на операційні процеси обробки подій кібербезпеки	69
2.1.1. Причинно-наслідне представлення впливу	69
2.1.2. Метрика втрати спостережності	71
2.1.3. Вплив на інцидентність і якість виявлення	72
2.1.4. Вплив на MTTD і MTTR	74
2.1.5. Інтегральне представлення та межі моделі	75
2.2. Схема управління активами з врахуванням динамічності та резервування інфраструктури	76
2.3. Дескриптивна модель формування методів покращення спостережності	85
2.3.1. Ідентифікація вразливих компонентів інфраструктури	86
2.3.2. Оцінювання ризиків та формування джерел невизначеності спостережності під час реагування	88
2.3.3. Результати ідентифікації ризиків	89
2.4. Методи обробки подій безпеки призначені для покращення спостережності інформації в ІКС	92
2.4.1. Контроль змін стану живлення та відновлення стану системи (Power status changes control)	92

2.4.2. Контроль доступності каналів зв'язку (Communication channel availability control)	92
2.4.3. Контроль аномалій оренди DHCP (DHCP leasing anomaly control) .	93
2.4.4. Контроль змін конфігурації обладнання (Hardware configuration changes control)	93
2.4.5. Контроль стану живлення мережевого сегмента (Network segment power status control)	93
2.4.6. Контроль цілісності та повноти журналів (Log data integrity control)	94
2.4.7. Контроль доступності хмарних агентів (Cloud agents uptime control)	94
2.4.8. Метод ідентифікації втрати спостережності	94
2.4.9. Фільтр динамізму активу	95
2.4.10. Контроль динамічного впливу	95
2.4.11. Метод застосування метрики відповідності захисту об'єкту профілю загроз	96
2.4.12. Метод пріоритизації операцій Threat Hunting як ручної перевірки наявності потенційних загроз.	97
2.4.13. Контроль достатнього рівня резервування критичних динамічних систем	97
2.4.14. Візуалізація та огляд розроблених методів покращення спостережності	98
Висновки до розділу	99
РОЗДІЛ 3. Розробка архітектури та прототипу технічної імплементації СИСТЕМИ СПОСТЕРЕЖНОСТІ ІКС ТА ЗМЕНШЕННЯ НЕВИЗНАЧЕНОСТІ у виявленні кіберінцидентів	101
3.1. Постановка вимог для розробки системи	101
3.1.1. Призначення та межі рішення.....	101

3.1.2. Розподіл функцій між готовими продуктами та власною розробкою	101
3.1.3. Технічний проєкт.....	102
3.1.4. Вимоги до даних та моделей.....	103
3.1.5. Вимоги до функцій (контролів) та інтеграції з SIEM.....	103
3.1.6. Вимоги до підтримки реагування (алгоритм декомпозиції та ізоляції)	104
3.2. Архітектура системи	105
3.2.1. Підсистема збору та аналізу подій, інцидентів безпеки (SIEM)	105
3.2.2. Підсистема активного реагування (EDR, NDR).....	108
3.2.3. Підсистема інвентаризації та злиття (SAM Core + Fusion).....	110
3.2.4. Модуль обрахунку динамізму	114
3.2.5. Модуль обрахунку дескриптора загроз	117
3.2.6. Підсистема візуалізації та звітності	120
3.3. Прототип технічного рішення.....	123
3.3.1. Принципи відкритої архітектури та розмежування «власна розробка / готові компоненти»	123
3.3.2. Апробаційний технологічний стек прототипу та обґрунтування вибору	124
3.3.4. Внутрішні потоки даних і сценарій роботи прототипу	125
3.3.5. Підсистема візуалізації та звітності в прототипі	128
Висновки до розділу	129
РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ СИСТЕМИ СПОСТЕРЕЖНОСТІ ІКС ТА ЗМЕНШЕННЯ НЕВИЗНАЧЕНОСТІ у виявленні кіберінцидентів.....	131
4.1. Мета та логіка експерименту	131
4.3. Експериментальний стенд.....	132

4.3. Дані та моделі, використані в експерименті.....	135
4.4. Обмеження експерименту	136
4.5. Підготовка експерименту	136
4.6. Сценарії експериментальної перевірки.....	137
4.7. Метрики та порядок оцінювання.....	140
4.8. Перебіг експерименту та фіксація результатів	144
4.9. Результати експерименту	147
4.9.1. Результати виявлення та структуризації втрати спостережності ...	149
4.9.2. Порівняння базового та пропонованого режимів за обсягом сигналів і хибнопозитивних спрацювань	150
4.9.3. Вплив на якість виявлення та середній час виявлення	151
4.9.4. Результати диференціації причин деградації	152
4.9.6. Результати пріоритезації на основі дескриптора загроз.....	153
4.9.7. Узагальнені результати	153
Висновки до розділу	154
ВИСНОВКИ.....	157
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	161
ДОДАТОК А	167
ДОДАТОК Б	169

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ADSL – Asymmetric Digital Subscriber Line / Асиметрична цифрова абонентська лінія

APT – Advanced Persistent Threat / Складна цільова (персистентна) загроза

ATT&CK – Adversarial Tactics, Techniques and Common Knowledge / База знань тактик і технік супротивника

CERT-UA – Computer Emergency Response Team of Ukraine / Урядова команда реагування на комп'ютерні надзвичайні події України

CMDB – Configuration Management Database / База даних керування конфігураціями

CNAPP – Cloud-Native Application Protection Platform / Платформа захисту хмарно-орієнтованих застосунків

DHCP – Dynamic Host Configuration Protocol / Протокол динамічної конфігурації вузла

DNS – Domain Name System / Система доменних імен

EDR – Endpoint Detection and Response / Виявлення та реагування на кінцевих точках

FQDN – Fully Qualified Domain Name / Повне доменне ім'я

GDPR – General Data Protection Regulation / Загальний регламент захисту даних Європейського Союзу

HLD – High-Level Design / Високорівневе архітектурне проектування

IDS – Intrusion Detection System / Система виявлення вторгнень

IPS – Intrusion Prevention System / Система запобігання вторгненням

IoC – Indicator of Compromise / Індикатор компрометації

IP – Internet Protocol / Протокол міжмережевої взаємодії

JSON – JavaScript Object Notation / Текстовий формат обміну структурованими даними

MAC – Media Access Control / Керування доступом до середовища передачі

MITRE – MITRE Corporation Knowledge Base / База знань корпорації MITRE

MTTD – Mean Time To Detect / Середній час виявлення інциденту

MTTR – Mean Time To Response / Середній час реагування на інцидент

NDR – Network Detection and Response / Виявлення та реагування в мережі

NGFW – Next-Generation Firewall / Міжмережевий екран наступного покоління

NMS – Network Management System / Система керування мережею

OKI – Об'єкти критичної інфраструктури

RAM – Random Access Memory / Оперативна пам'ять

SAM – Security Asset Management / Керування активами безпеки

SD-WAN – Software-Defined Wide Area Network / Програмно-керована глобальна мережа

SIEM – Security Information and Event Management / Система керування подіями та інцидентами безпеки

SOC – Security Operations Center / Операційний центр кібербезпеки

SSO – Single Sign-On / Єдина автентифікація

TH – Threat Hunting / Проактивний пошук загроз

TPM – Trusted Platform Module / Довірений платформний модуль

UPS – Uninterruptible Power Supply / Джерело безперебійного живлення

UTP – Unshielded Twisted Pair / Неекранована вита пара

VLAN – Virtual Local Area Network / Віртуальна локальна мережа

VPN – Virtual Private Network / Віртуальна приватна мережа

WAF – Web Application Firewall / Міжмережевий екран веб-застосунків

ЦОД – Центр обробки даних / Data Center

ДБЖ – Джерело безперебійного живлення / Uninterruptible Power Supply

ІКС – Інформаційно-комунікаційна система / Information and Communication System

КСЗІ – Комплексна система захисту інформації / комплексна система організаційно-технічних заходів захисту

НД ТЗІ – Нормативні документи з технічного захисту інформації / Regulatory documents on technical information protection

ВСТУП

Актуальність теми. Процеси збору та аналізу подій та процеси моніторингу та реагування на інциденти в операційному центрі кібербезпеки (Security Operations Center, SOC) залежать від безперервності надходження телеметрії, узгодженості контексту активів та стабільності інфраструктурних компонентів. За умов воєнних впливів і деградації цивільної інфраструктури виникають систематичні порушення енергоживлення та зв'язку, що спричиняє переривчастість журналювання, затримки доставлення подій, фрагментацію видимості та прискорення динаміки змін складу інфраструктури. З точки зору теорії керування, існує класична проблема втрати спостережності інформації. В даному дослідженні спостережність інформації трактується як характеристика системи, що визначає ступінь можливості відновлення її внутрішніх станів на основі даних про зовнішні вихідні сигнали [1]. У цих умовах традиційні підходи кореляції та реагування в підсистемах управління подіями та інцидентами безпеки формують підвищений ризик некоректних висновків через змішування технічної недоступності компонентів і можливих зловмисних впливів, а також через втрату контексту щодо складу, критичності й топології активів.

Проблемам збору, обробки та аналізу інформації в комп'ютерних системах присвячено дослідження О.В.Потія, О.О.Бакалинського, Ф.О.Коробейнікова, Д.Форсберга [2-17]. Зокрема в [3] розглядається механізми побудови організаційного контуру функціонування центрів кібербезпеки та побудови керованих моделей кіберстійкості. В [7] досліджуються моделі й методи визначення проєктних характеристик систем управління інформаційною безпекою, тобто у напрямі формалізації керованості та архітектурних параметрів безпекових систем; В [13-14] висвітлюються питання цілей кібербезпеки та кіберрезильєнтності, що безпосередньо корелює з проблематикою стійкості, спостережності та збереження керованості в умовах деградації середовища. В [17] наведено розвиток підходу до технічних метрик ефективності SOC, формалізуючи вимірювання результативності операцій безпеки, що є релевантним для побудови дескриптивної моделі впливів воєнних факторів на операційну діяльність.

Формалізація спостережності як керованої властивості та побудова спеціального класу контролів деградації телеметрії є необхідною передумовою відтворюваності операційних рішень і коректної пріоритезації дій в умовах неповноти інформації про стан та активність системи. Відсутність формалізованого апарату, що дозволяє розглядати «втрату спостережності» як вимірюваний стан інформаційної системи, відсутність можливості враховувати деградацію телеметрії у процедурах SOC на операційному рівні та інтегрувати відповідні методи у вендор-агностичну архітектуру SOC-платформи без необхідності заміни базових інструментів є складовими визначеної проблематики.

Дисертаційне дослідження спрямоване на розробку та розвиток існуючих методів обробки подій безпеки в контексті умов погіршеної спостережності інформаційних систем спричиненої деградацією інфраструктури, що узгоджується з прикладними напрямками забезпечення стійкості кіберзахисту розподілених інформаційних систем, підвищення якості телеметрії та відтворюваності рішень під час реагування на інциденти в середовищах із переривчастою зв'язністю та частково некерованими компонентами.

Актуальним науковим завданням є розробка методів збору та аналізу подій безпеки адаптованих до умов непрозорого середовища та специфічних військових впливів.

Мета і завдання дослідження. Метою роботи є підвищення ефективності процесів збору та аналізу інформації в комп'ютерних системах управління подіями безпеки в умовах деградації інфраструктури інформаційно-комунікаційних систем шляхом розширення існуючих процесів збору та аналізу подій безпеки.

Для досягнення поставленої мети сформовано наступні завдання:

1. ідентифікувати існуючі методи обробки та аналізу подій безпеки в комп'ютерних системах управління подіями;

2. визначити ключові фактори впливу повномасштабної війни на процеси обробки та аналізу подій в комп'ютерних системах управління подіями безпеки;
3. оцінити ефективність існуючих підходів до протидії втраті спостережності в умовах деградації інфраструктури та інших специфічних факторів військового часу;
4. розробити формалізовану модель впливу деградації інфраструктури на стан спостережності інформації та якість процесів в комп'ютерних системах управління подіями безпеки;
5. розробити методи протидії негативним впливам спостережності інформації військового часу в комп'ютерних системах управління подіями безпеки;
6. розробити вимоги та архітектуру технічного рішення покращення спостережності комп'ютерної системи, що імплементує розроблені методи;
7. визначити ключові технічні компоненти експериментального стенду для перевірки ефективності розроблених методів в комп'ютерній системі покращення спостережності та експериментально підтвердити ефективність розроблених методів;

Об'єктом дослідження процеси збору, аналізу інформації про події та інциденти, та процеси прийняття рішень в операційних центрах кіберзахисту.

Предметом дослідження є методи збору та аналізу інформації в SOC спрямовані на підвищення спостережності інформаційних систем.

Методи дослідження - функціональний і порівняльний аналіз застосовано для виконання завдань Розділу 1, зокрема дослідження факторів впливу деградації інфраструктури на показники ефективності операційних центрів безпеки, існуючих методів протидії. Математичне, комп'ютерне моделювання та формалізація широко застосовуються в Розділі 2 для формалізації стану втрати спостережності, побудови дескриптивної моделі впливу деградації інфраструктури на операційні метрики, опису активу як сукупності атрибутів у

межах управління безпековими активами, визначення атрибутів динамізму, дескриптора загроз, а також для експериментального відтворення сценаріїв масової втрати електроживлення, деградації каналів зв'язку, відновлення після деградації та накладання зловмисної активності на фон технічної недоступності. Методи синтезу та архітектурного проєктування застосовано в Розділі 3 для розробки вимог і відкритої модульної архітектури технічного рішення, що імплементує запропоновані методи підвищення спостережності. Експериментальний метод та імітаційне моделювання застосовується в Розділі 4 для побудови стенду та проведення практичного дослідження ефективності розробленої методології.

Наукова новизна здобутих результатів:

1. Вперше розроблено постановку задачі підвищення спостережності інформації у контексті деградації інфраструктури, у якій «втрата спостережності» визначається як стан системи, за якого зменшується повнота та/або достовірність телеметрії до рівня, що порушує коректність виконання щонайменше одного класу процедур операційного центру кіберзахисту (виявлення, розслідування, атрибуція, реагування), а перехід у такий стан описується вимірюваними ознаками доступності джерел подій і узгодженості інвентарних даних;
2. Дістав подальшого розвитку метод атрибутивного профілювання активів завдяки запропонованому вектору атрибутів, релевантних для оцінювання спостережності та ризиків інтерпретації телеметрії за умов деградації інфраструктури;
3. Вперше запропоновано багатоконтурну архітектуру спостережності, в якій виділено контури інвентаризації та злиття даних про активи, аналітики подій/інцидентів, активного реагування, атрибутивного профілювання та обчислення правил/метрик, а також візуалізації та звітності прототипу, що дозволило розробити прототип відповідного технічного рішення.
4. Розроблено методологію орієнтовану на корекцію процесів обробки сигналів в операційних центрах кіберзахисту, спрямовану на виявлення та

врахування деградації спостережності, як необхідної умови коректної інтерпретації сигналів про кіберзагрози за умов воєнних впливів;

Особистий внесок здобувача. Наукові результати дослідження, які виносяться на захист, одержані автором самостійно.

Практичне значення одержаних результатів. Практичне значення одержаних результатів полягає у можливості використання розробленої методології, прототипу і архітектурних вимог для підвищення ефективності процесів збору, обробки та аналізу подій безпеки в умовах деградації інфраструктури, неповноти телеметрії та обмеженої спостережності. Розбудова контекстно-залежних правил кореляції призводить до зниження кількості хибних інтерпретацій і відокремлення технічної деградації від потенційної активності загрозового агента. Результати можуть бути використані під час проєктування та модернізації технологічних платформ SOC, удосконалення процедур реагування, оцінювання достатності резервування критичних компонентів, планування операційних процедур кіберзахисту.

Зв'язок роботи з науковими програмами, планами, темами.

Тематика дисертаційної роботи відповідає пріоритетним напрямкам розвитку науки і техніки в Україні. Робота виконувалась відповідно до плану наукових досліджень Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, зокрема в рамках НДР “Кіберризика та кіберзахищеність топології розподілених інформаційних систем в глобальному кіберпросторі”, (державний рег. № 0123U102744) та «Розроблення науково-обґрунтованих критеріїв та принципів побудови системи кіберзахисту об’єктів атомної енергетики», державний рег. № 0123U100909.

Апробація результатів дослідження. Результати дисертаційного дослідження пройшли всебічну апробацію як у науковому середовищі, так і на експериментальному стенді. Здобуті напрацювання були представлені на низці науково-практичних заходів, зокрема: ITS-2023: Information Technologies and

Security (результати опубліковані в CEUR WS), IV та V науково-практичній конференції «Безпека енергетики в епоху цифрової трансформації», Науково-практичній конференції «Штучний інтелект і безпека».

Публікації. Основні наукові положення та результати дисертаційної роботи підлягають висвітленню у фахових наукових публікаціях і матеріалах науково-практичних заходів відповідно до вимог атестації здобувача наукового ступеня.

Обсяг та структура роботи. Дисертація складається зі вступу, чотирьох розділів, висновків, переліку використаних джерел та додатків. У першому розділі проаналізовано вплив сучасних умов функціонування інформаційно-комунікаційних систем на спостережність інформації в комп'ютерних системах управління подіями безпеки, визначено ключові фактори військового часу, що порушують повноту, своєчасність і достовірність телеметрії, а також оцінено наявні підходи до протидії втраті спостережності, обґрунтовано актуальність та ідентифіковано рамку досліджуваної проблеми. У другому розділі розроблено методологічний апарат підвищення спостережності, включно з дескриптивною моделлю впливу деградації інфраструктури, атрибутивним профілюванням активів, метриками та правилами контролю втрати спостережності, а також принципами диференціації технічної деградації й потенційної активності загрозового агента. У третьому розділі сформовано вимоги та архітектуру технічного рішення, що імплементує запропоновані методи у вигляді відкритої модульної системи, визначено склад підсистем, інтеграційні вимоги до компонентів технологічної платформи. У четвертому розділі наведено результати експериментальної перевірки ефективності розроблених методів, виконано порівняння базового режиму обробки подій із режимом, що використовує запропоновану методологію, та підтверджено зменшення кількості хибних інтерпретацій, підвищення якості класифікації і покращення пріоритезації подій за умов обмеженої спостережності.

Застосування інструментів штучного інтелекту при виконанні дослідження. Інструмент ChatGPT – GPT-5.5 використовувався при розробці

тексту дисертаційної роботи для перевірки орфографії, стилістики викладення та оформлення тексту та відповідного редагування. Автор виконав перевірку, редагування та підтвердження будь-яких правок, виконаних інструментом, і бере на себе повну відповідальність за якість, зміст та форму викладеного матеріалу.

РОЗДІЛ 1. АНАЛІЗ ВПЛИВУ СУЧАСНИХ УМОВ ФУНКЦІОНУВАННЯ ІКС НА СПОСТЕРЕЖНІСТЬ ІНФОРМАЦІЇ. ОГЛЯД ІСНУЮЧИХ МЕТОДІВ ТА АЛГОРИТМІВ ПРОТИДІЇ.

1.1. Огляд існуючих методів обробки та аналізу інформації в комп'ютерних системах управління подіями безпеки

Центральним технологічним компонентом SOC зазвичай є система управління інформацією та подіями безпеки (Security Information and Event Management, SIEM). Її функції охоплюють отримання подій із різномірних джерел, приведення записів до спільної структури, збереження, пошук, кореляцію, формування оповіщень і надання аналітику контексту для розслідування [18]. SIEM взаємодіє із системами виявлення вторгнень, засобами захисту кінцевих точок, платформами кіберрозвідки, реєстрами активів і системами автоматизації реагування. Комп'ютерну систему управління подіями безпеки доцільно розглядати як сукупність взаємопов'язаних підсистем збору, обробки, зберігання, аналізу та інтерпретації даних.

Існуючі методи можуть бути систематизовані за рівнями перетворення інформації [19] [18] [20] [21] [22] [23]:

- збір та попередня обробка телеметрії;
- детерміноване виявлення визначених ознак;
- агрегація та кореляція подій;
- статистичний і поведінковий аналіз;
- причинно-наслідкове моделювання;
- семантичне збагачення;
- оцінювання ризику;
- ретроспективний аналіз.

1.1.1. Збір та попередня обробка телеметрії

Первинним етапом є централізоване отримання даних від джерел. Збір може здійснюватися шляхом передачі журналів джерелом, періодичного опитування, використання програмних агентів, розташованих на об'єктах ІКС, отримання повідомлень через програмні інтерфейси або перехоплення

мережевого трафіку. На даному рівні застосовуються методи обробки, спрямовані перш за все на дотримання цілісності даних. Їхнє призначення полягає у зменшенні втрат телеметрії та забезпеченні відтворюваності подій. Для коректної побудови часових послідовностей відбувається синхронізація системного часу джерел, оскільки розбіжності часових міток можуть змінювати встановлений порядок дій і спричиняти помилкову кореляцію.

Отримані записи проходять синтаксичний розбір. Під час розбору неструктурований або частково структурований запис розділяється на поля, такі як час, джерело, суб'єкт дії, об'єкт, тип операції, результат, мережеві адреси, ідентифікатори процесів, коди помилок та інші параметри. Правила розбору можуть бути побудовані на регулярних виразах, формальних граматиках, схемах серіалізації або програмних перетворювачах.

Після розбору відбувається нормалізація. Нормалізація полягає у відображенні різних подань семантично однакових подій на спільну модель. Наприклад, успішна автентифікація в різних операційних системах може мати різні коди, назви полів і формати запису, але після нормалізації подається єдиним типом події з узгодженими атрибутами суб'єкта, вузла, часу та результату.

Одночасно, або після нормалізації відбувається категоризація, тобто віднесення події до визначеного класу. Категоризація утворює проміжний семантичний рівень між форматом конкретного виробника та аналітичною логікою SOC.

До попередньої обробки також належать фільтрація, дедуплікація та агрегація. Фільтрація вилучає записи, які не мають аналітичної цінності в заданому контексті. Дедуплікація усуває повторні копії однієї події, отримані від кількох колекторів або внаслідок повторного передавання. Агрегація об'єднує однорідні події за часовим інтервалом і набором атрибутів. Зменшення обсягу даних на цьому етапі не усуває атрибути, необхідні для відновлення послідовності дій. Правила зменшення даних визначаються з урахуванням подальших методів кореляції [19].

1.1.2. Детерміновані методи виявлення

Найпоширенішим класом методів виявлення інцидентів є детерміновані методи, у яких умови виявлення задаються явно. Результат такого методу однозначно визначається значеннями полів події, станом системи та параметрами правила. Найпростішим різновидом є сигнатурне зіставлення. Подія або об'єкт порівнюється з визначеним шаблоном, що описує відому шкідливу активність. Шаблоном може бути контрольна сума або результат hash-функції по відношенню до файлу, мережева адреса, доменне ім'я, фрагмент команди, послідовність байтів, назва процесу або комбінація атрибутів. Технічні значення, безпосередньо придатні для такого зіставлення, називають індикаторами компрометації (Indicator of Compromise, IOC) [18].

Перевагами сигнатурного методу є визначеність результату, низька обчислювальна складність і прозорий причинно-наслідковий зв'язок. Обмеження полягає в залежності від попереднього знання конкретної ознаки. Зміна адреси, файлу, параметра команди або способу виконання може зробити сигнатуру нефункціональною. Атомарний індикатор без контексту не визначає, чи є відповідна дія частиною підтвердженого інциденту. Цінність окремих ІоС обмежується коротким строком актуальності, тоді як поведінкові характеристики та контекст мають тривалішу аналітичну цінність [18].

Порогові методи визначають аномальний стан за кількістю або частотою подій. Правило спрацьовує, якщо за заданий інтервал часу кількість невдалих автентифікацій, мережевих з'єднань, звернень до ресурсу або змін конфігурації перевищує встановлений поріг. Метод застосовується для виявлення перебору паролів, сканування, масового завантаження даних, розподілених атак на доступність і повторюваних помилок засобів захисту – та інших атак, характерною ознакою яких є масовість події на фоні звичайної активності.

Логічні правила поєднують кілька умов операціями кон'юнкції, диз'юнкції та заперечення. Наприклад, подія може вважатися підозрілою лише за одночасного виконання таких умов: використано адміністративний обліковий

запис, вхід здійснено з нетипового вузла, операція відбулася поза визначеним часовим інтервалом і після неї зафіксовано зміну конфігурації.

Перевагою детермінованих правил є їхня придатність для формального тестування. Для кожного правила можна визначити вхідні умови, очікуваний результат і контрольний набір подій. Основними недоліками є витрати на супроводження, залежність від повноти телеметрії та поступове зниження відповідності правила реальній інфраструктурі внаслідок зміни конфігурації [18].

1.1.3. Методи комплексної обробки подій

Комплексна обробка подій (Complex Event Processing, CEP) призначена для виявлення складних станів у потоках даних на підставі часових, логічних і причинних зв'язків між простими подіями. На відміну від перевірки одиничного запису, CEP оперує часовими вікнами, послідовностями, відсутністю очікуваних повідомлень, повтореннями та станами об'єктів [20].

Типовий шаблон CEP може визначати, що подія (A) має передувати події (B), після чого протягом визначеного інтервалу повинна виникнути подія (C). Додатковою умовою може бути належність усіх подій одному користувачу, вузлу, сеансу або мережевому сегменту. Такі конструкції придатні для виявлення багатокрокових дій: початкового доступу, запуску процесу, отримання привілеїв і встановлення механізму закріплення. CEP може виявляти не лише наявність, а й відсутність події. Наприклад, припинення надходження контрольних повідомлень від джерела журналювання протягом визначеного часу може бути сформоване як окрема подія втрати телеметрії. У потоковій архітектурі низькорівневі записи фільтруються, очищуються, нормалізуються та зіставляються з моделями складних подій у реальному часі. Практичними обмеженнями CEP є необхідність керування станом для великої кількості паралельних об'єктів, обробка запізнених повідомлень і вибір розміру часових вікон. Надто коротке вікно призводить до пропуску повільних послідовностей, а надто довге - до утворення випадкових зв'язків між незалежними діями.

Результат також залежить від політики обробки подій, які надійшли не в порядку їх виникнення [20].

1.1.4. Методи агрегації та кореляції оповіщень

Кореляція є основним методом переходу від множини низькорівневих подій до інформаційного представлення інциденту. Метод визначає, які записи або оповіщення пов'язані між собою та мають аналізуватися як єдина послідовність. У роботі [21] кореляцію оповіщень визначено як процес побудови стислого високорівневого подання спроб вторгнення на основі результатів одного або кількох засобів виявлення. Метод включає нормалізацію, попередню перевірку, об'єднання споріднених оповіщень, встановлення зв'язків і формування сценаріїв. Атрибутивна кореляція встановлює зв'язок за подібністю атрибутів. Для кожної пари подій може бути визначена функція подібності. Події об'єднуються, якщо значення функції перевищує поріг. Часова кореляція враховує взаємне розташування подій у часі. Вона засновується на фіксованих вікнах, варіативних часових інтервалах або статистичному оцінюванні часової близькості. Метод застосовується для виявлення атак, компоненти якого очікуються протягом визначеного часового інтервалу. Просторова кореляція використовує належність подій до спільного вузла, сегмента, облікового запису, прикладного сервісу або географічного майданчика.

Кореляція на основі передумов і наслідків подає кожен клас атаки через множину умов, необхідних для її виконання, та множину станів, що можуть виникнути після виконання. Дві події пов'язуються, якщо наслідок першої задовольняє передумову другої. В роботі [22] запропонували формальний підхід до побудови сценаріїв атак саме на основі такого зв'язку. Метод дозволяє встановлювати причинно обґрунтовану послідовність і відрізняється від простого об'єднання за часовою близькістю.

Кореляція за передумовами та наслідками придатна для виявлення багатокрокових атак, але потребує формалізованих моделей технік і станів системи. Якщо модель не містить нової техніки або альтернативного способу

досягнення стану, відповідний зв'язок не буде встановлений. Помилки в даних про активи, склад інфраструктури та порушення спостережності також можуть спричинити хибне відкидання коректної послідовності.

1.1.5. Кластеризація та аналіз першопричин

Кластеризація є методом автоматичного поділу множини подій або оповіщень на групи, внутрішньо однорідні за обраними ознаками. На відміну від правил із наперед визначеними умовами, кластеризація може виявляти структуру даних без попереднього переліку всіх класів. До ознак кластеризації можуть бути віднесені практично всі атрибути подій. Результатом є групи подібних спрацювань, які можуть відповідати одному класу сигналу про інцидент.

В роботі [23] запропоновано кластеризацію оповіщень для встановлення їхніх стійких першопричин. Дослідження реальних даних показало, що переважна частина оповіщень може бути зумовлена обмеженою кількістю постійних причин, зокрема помилками конфігурації. Усунення цих причин зменшує навантаження на аналітиків не шляхом приховування оповіщень, а шляхом ліквідації умов їх повторного виникнення.

Кластеризація в системах управління подіями безпеки може використовуватися для:

- групування однотипних оповіщень;
- виявлення кампаній або координованої активності;
- побудови профілів постійного фоновому шуму;
- пошуку невідомих повторюваних шаблонів;
- визначення правил, що генерують непропорційно велику кількість спрацювань;
- підготовки вибірок для подальшого маркування аналітиками.

Недоліком є відсутність однозначної семантичної інтерпретації кластера. Алгоритм визначає статистичну подібність, але не встановлює автоматично, чи є її причиною атака, технічна несправність або нормальний технологічний

процес. Для практичного використання необхідна експертна перевірка сформованих груп.

1.1.6. Статистичні методи та виявлення аномалій

Виявлення аномалій полягає у пошуку спостережень, які істотно відрізняються від моделі нормального стану. Відповідно до систематизації [24], розрізняють точкові, контекстні та колективні аномалії. Точкова аномалія визначається властивостями одного спостереження. Контекстна аномалія релевантна лише за певних умов часу, місця або стану. Колективна аномалія визначається структурою групи спостережень, кожне з яких окремо може бути допустимим.

В процесах моніторингу подій безпеки точковою аномалією може бути виконання нетипового процесу. Контекстною — адміністративна дія в нетиповий час або з нового пристрою. Колективною — послідовність низькоінтенсивних мережевих з'єднань, яка в сукупності відповідає повільному скануванню.

Статистичні методи формують розподіл або набір характеристик нормальної активності. Для числової ознаки можуть оцінюватися середнє значення, дисперсія, квантілі, сезонність або частотний розподіл. Подія визнається аномальною, якщо її значення виходить за допустимий інтервал або має низьку ймовірність відповідно до моделі. Методи часових рядів застосовуються до кількості автентифікацій, обсягу трафіку, кількості запущених процесів, швидкості створення файлів або частоти звернень до сервісу. Вони враховують тренд, періодичність і сезонні коливання. Перевагою статистичних методів є можливість виявлення відхилень, для яких не створено сигнатуру. Недоліками є чутливість до вибору періоду навчання, наявність легітимних рідкісних подій і зміна нормального режиму роботи. Даний метод має істотний супровідний ризик - нерозпізнана зловмисна активність в навчальних даних може бути включена до моделі норми.

1.1.7. Причинно-наслідні та графові методи

Графові методи подають об'єкти інфраструктури, події, облікові записи, процеси, вразливості та техніки атак у вигляді вершин, а відношення між ними — у вигляді ребер. Ребро може позначати мережеву доступність, запуск процесу, використання облікового запису, передавання файлу, залежність сервісу або причинний зв'язок між подіями. Граф атаки описує можливі переходи між станами системи. Для його побудови використовуються дані про топологію, конфігурацію, права доступу та вразливості. Отримані від засобів моніторингу події відображаються на відповідні вершини або переходи. Якщо послідовність спостережень відповідає шляху в графі, система формує гіпотезу щодо сценарію атаки [22].

Кореляція на основі графів не обмежується точним збігом усіх спостережень із моделлю. Деякі алгоритми допускають формування гіпотези щодо відсутньої події, якщо попередній і наступний стани узгоджуються з допустимим шляхом. Якість графової реконструкції визначається актуальністю моделі інфраструктури. Відсутній актив, неправильний зв'язок або застаріла інформація про доступність сервісу змінюють множину допустимих шляхів. Графові методи потребують інтеграції з процесами інвентаризації активів, керування конфігураціями та вразливостями.

1.1.8. Методи контекстного збагачення

Контекстне збагачення полягає у приєднанні до події додаткових відомостей, які не містилися в первинному записі, але необхідні для її інтерпретації. Джерелами контексту є реєстри активів, системи керування конфігураціями, каталоги користувачів, результати сканування вразливостей, географічні дані, відомості про критичність сервісів і кіберрозвідувальна інформація.

- Подія мережевого з'єднання після збагачення може містити:
- роль і критичність вузла;
- власника системи;
- належність до сегмента;

- операційну систему;
- наявні вразливості;
- статус засобів захисту;
- репутаційні відомості про зовнішню адресу;
- відповідність поведінковій техніці;
- попередні пов'язані оповіщення.

Контекстне збагачення зменшує неоднозначність. Однакова подія має різний пріоритет для тестового вузла та для сервера автентифікації. Водночас некоректний контекст може систематично спотворювати результати. Тому для приєднаних даних необхідно зберігати атрибути джерела, час останнього підтвердження та рівень довіри [18].

1.1.9. Методи ретроспективного аналізу та реконструкції інциденту

Ретроспективний аналіз виконується після отримання первинного оповіщення або нової інформації про загрозу. Метою є встановлення початкової точки компрометації, тривалості активності, переліку об'єктів і повної послідовності дій. Основним методом є пошук за атрибутами та часовими інтервалами. Аналітик або автоматизований модуль формує запити за користувачем, вузлом, адресою, процесом, файлом, сеансом чи технікою. Результати впорядковуються за часом і об'єднуються в часову шкалу. Метод розширення контексту передбачає ітеративний перехід від одного об'єкта до пов'язаних. Від підозрілого процесу здійснюється перехід до батьківського процесу, користувача, мережових з'єднань, створених файлів та інших вузлів, на яких виявлено той самий об'єкт. Таке дослідження природно подається у формі графа походження даних [25].

Пошук за новими індикаторами дозволяє повторно аналізувати історичні дані після отримання відомостей про кампанію або шкідливе програмне забезпечення. Цінність методу залежить від строку зберігання, повноти журналів і збереження первинних атрибутів. Метод перевірки гіпотез полягає у формулюванні припущення щодо механізму інциденту та визначенні подій, які мають підтвердити або спростувати його. На відміну від послідовного

перегляду всіх записів, цей підхід спрямовує пошук на конкретні залежності. Комп'ютерна система може підтримувати перевірку шляхом автоматичного формування запитів і зіставлення результатів із моделлю сценарію. Актуальна редакція рекомендацій NIST щодо реагування пов'язує процеси виявлення, реагування та відновлення із загальним керуванням ризиками [25].

1.2. Огляд специфічних впливів на спостережність інформації в системах управління подіями безпеки в умовах повномасштабної війни

1.2.1. Руїнування енергетичної та телекомунікаційної інфраструктури

Фізичне пошкодження енергетичної та телекомунікаційної інфраструктури належить до зовнішніх чинників, які безпосередньо порушують операційну роботу операційних центрів кібербезпеки. Унаслідок кінетичних ударів по енергосистемі України наприкінці 2022 р. та на початку 2023 р. відключення електропостачання тривали від кількох годин до кількох діб. За таких умов знижувалась доступність центрів обробки даних, мережевих вузлів і джерел телеметрії, переривався збір подій, зростало навантаження на резервні підсистеми та погіршувалась передача даних. Масштаб необхідного резервування відображають дані оператора Kyivstar: станом на 2024 р. на базових станціях було розгорнуто 2322 дизель-генератори та понад 115 тис. акумуляторних батарей [26][27].

Для SOC пошкодження енергетичної та телекомунікаційної інфраструктури означає часткову втрату спостережності й розрив цілісного контуру моніторингу [28]. За відсутності живлення або зв'язку окремі сегменти мережі фізично ізолюються, події з них не надходять у реальному часі, а сенсори втрачають синхронізацію з центральними консолями. Аварійна маршрутизація та перехід на альтернативні, зокрема супутникові, канали часто супроводжуються зменшенням пропускну здатності й збільшенням часу реагування. Протидія включає резервування електроживлення та зв'язку, контролі виявлення втрати живлення або мережевої доступності, а також доповнення інвентаризаційної моделі відомостями про динамічність активів і їх

залежність від енергетичних ресурсів. В українських умовах застосовувались поєднання резервних джерел живлення, супутникових каналів, перенесення сервісів до хмарних середовищ і сегментації інфраструктури віртуальних приватних мереж (Virtual Private Network, VPN) [26][29].

Ретроспективний аналіз вибірки діючих SOC, наведений у [26], фіксує вимірюване погіршення операційних показників під час масових відключень електропостачання. У червні–серпні 2024 р. середній час реагування на інцидент (Mean Time To Response, MTTR) був на 24 % більшим, ніж у грудні 2023 р. – лютому 2024 р., і на 26 % більшим, ніж у грудні 2024 р. – лютому 2025 р. Середній час виявлення інциденту (Mean Time To Detect, MTTD) зріс відповідно на 425 % і 412 %, тоді як доступність технологічної платформи SOC зменшилась приблизно на 7 %. Зміни збігалися з періодами зовнішніх інфраструктурних обмежень і спостерігались у кількох SOC, тому їх не можна пояснити лише особливостями внутрішньої організації окремого підрозділу [26][36] [29] [37].

1.2.2. Окупація та втрата об'єктів ІТ-інфраструктури

Окупація територій і розміщених на них об'єктів ІТ-інфраструктури утворює окремий клас загроз, характерний для повномасштабної війни зі змінною лінією бойового зіткнення. У мирних умовах центри обробки даних, мережеві вузли та кінцеві точки переважно залишаються під фізичним контролем власника. Під час бойових дій актив може бути захоплений у працездатному стані або фізично знищений. Захоплений сегмент мережі може використовуватися для збереження доступу та подальшого просування в інфраструктурі. Із 2014 р. російські сили захоплювали вузли зв'язку й центри обробки даних на окупованих територіях та інтегрували їх до власної телекомунікаційної системи. Після 2022 р. регіональний трафік примусово спрямовувався через мережі Miranda Media/Rostelecom, що створювало технічні умови для його контролю та цензурування [26][30][31].

У роботі SOC захоплення інфраструктури означає одночасну втрату спостережності та довіри до даних із відповідної зони. Канали зв'язку,

ідентичності вузлів, журнали подій і засоби віддаленого керування більше не можуть вважатися надійними без додаткового підтвердження. Частину обладнання оператори навмисно від'єднували або знищували, щоб запобігти його використанню супротивником. Паралельно державні реєстри та критичні сервіси прискорено переносилися до хмарних середовищ, розміщених поза зонами безпосереднього ризику [26][30].

За втрати фізичного контролю порушується весь домен довіри. Атрибути автентичності, зокрема MAC- та IP-ідентифікатори, сертифікати й модуль довіреної платформи (Trusted Platform Module, TPM), а також індикатори компрометації (Indicators of Compromise, IoC) не можуть використовуватися як достатня підстава для висновку про стан активу. У період маневрених бойових дій у лютому–червні 2022 р. для окремих географічних зон застосовувався принцип *treat-as-compromised*. Особливу небезпеку становлять довірені міжсегментні з'єднання: *site-to-site VPN*, програмно-конфігурована глобальна мережа (*Software-Defined Wide Area Network, SD-WAN*), системи єдиного входу (*Single Sign-On, SSO*), агенти моніторингу та засоби реплікації резервних копій. За збереження таких зв'язків захоплений сегмент може стати каналом латерального переміщення до центральної інфраструктури [26][32].

1.2.3. Кадрова криза

Дефіцит персоналу обмежує спроможність SOC підтримувати заданий режим роботи під час повномасштабної війни. До 2022 р. українська ІТ-галузь і сфера кібербезпеки вже відчували нестачу фахівців, характерну також для глобального ринку. Евакуація, еміграція, зміна структури зайнятості, мобілізація та прямі втрати додатково зменшили кількість досвідчених працівників, доступних для роботи в SOC [33] [26]. У 2023–2024 рр. дефіцит персоналу, пов'язаний із воєнними обставинами, фіксували 67–74 % українських організацій. На глобальному рівні станом на 2025 р. близько 60 % команд кібербезпеки залишалися недоукомплектованими. Найскладніше замінювати фахівців рівня *Senior* та архітекторів безпеки, оскільки їх підготовка потребує тривалого набуття практичного досвіду [33] [26]. За меншої

чисельності команди зростає індивідуальне навантаження, збільшується тривалість аналізу й реагування, скорочується глибина розслідувань і охоплення загроз. Подібний вплив очікуваний і для інших військових конфліктів, у яких порушується стабільність кадрового забезпечення кібербезпеки [26] [32].

1.2.4. Фактор кібервійни

Повномасштабна війна супроводжується збільшенням інтенсивності операцій державних і пов'язаних із державою загрозливих агентів. З боку російської федерації діють організовані угруповання класу розвиненої сталої загрози (Advanced Persistent Threat, APT), активність яких проти України простежується з 2014 р., а у 2022–2023 рр. набула значно більшого масштабу. Кількість інцидентів різної складності зросла; станом на 2025 р. Україна посідала друге місце у світі за рівнем кіберзлочинності. На референсних інфраструктурах обсяг подій, які потребували аналізу та реагування SOC, збільшився приблизно у 2,5 раза [34] [26]. Після ескалації бойових дій в Ізраїлі у жовтні 2023 р. кількість звернень до національних кіберцентрів зросла приблизно з 50 до понад 500 на добу, а кількість активних APT-груп подвоїлася [35] [26]. Окремий клас становлять кібероперації, синхронізовані з кінетичними діями. 24 лютого 2022 р. було порушено роботу супутникової мережі ViaSat, атаковано інфраструктуру GigaTrans і приблизно на 15 год частково виведено з ладу мережу Укртелекому. У таких операціях застосовувалось спеціалізоване шкідливе програмне забезпечення Industroyer2, CaddyWiper і Pterodo; частка атак на критичну інфраструктуру зросла з 20 % у 2021 р. до 40 % у 2022 р.

За незмінного або скороченого ресурсного забезпечення SOC опрацьовує більше інцидентів, складніші послідовності подій і ширший перелік завдань реагування.

1.3. Аналіз загроз та ризиків для ІКС, пов'язаних з атаками на енергосистему

Для інформаційно-комунікаційної системи, що функціонує в державі з цілеспрямовано атакованою та суттєво пошкодженою енергосистемою, виникає сукупність загроз, безпосередньо пов'язаних із перервами електропостачання.

Реалізація цих загроз формує ризики для доступності, керованості та відновлюваності системи [46].

1.3.1. Недоступність та простій бізнес-сервісів та додатків, відключення обладнання та систем.

Найбільш безпосереднім наслідком відключення електропостачання для ІКС є зупинка частини обладнання, сервісів і прикладних систем. Відмова окремого компонента може порушити залежні функції та спричинити простій усієї системи, включно з прямими втратами через недоотриманий прибуток. Після повернення живлення автоматичний запуск не гарантує повного й коректного відновлення сервісу: окремі компоненти можуть залишитися недоступними або перейти в неузгоджений стан [46].

1.3.2. Необхідність додаткових витрат ресурсів команд підтримки та безпеки.

Відновлення сервісів після аварійного знеструмлення потребує додаткової участі команд технічного супроводу. У великих географічно розподілених системах окремо контролюються перерви в надходженні журналів подій. Припинення передавання безпекової телеметрії за звичайних умов може бути ознакою інциденту й вимагати розслідування. Під час масових відключень такі стани виникають одночасно для значної кількості джерел, через що фахівці інформаційної безпеки витрачають ресурси на перевірку технічних відмов, які зовні подібні до проявів атаки [46].

1.3.3. Відключення контролів безпеки

У географічно розподілених і структурно складній ІКС окремі засоби безпеки можуть бути розміщені на майданчиках без достатнього резервування електроживлення. У такій конфігурації основні бізнес-компоненти інколи продовжують роботу, тоді як один або кілька контролів уже недоступні. Незастосування контролю зменшує обсяг доступної телеметрії, утворює ділянку обмеженої спостережності та послаблює захист відповідного компонента системи [46][18] [38][39][40].

1.3.4. Погіршення спостережності внаслідок перерв у постачанні журналів.

У розподілених інформаційно-комунікаційних системах (ІКС) доставка журналів подій до централізованого колектора (log collector) є залежною від доступності трьох компонентів: клієнтської системи, каналу зв'язку та самого колектора. В умовах деградації інфраструктури кожен із цих компонентів може бути тимчасово недоступним, що призводить до переривання потоку телеметрії. За таких умов відсутність подій від окремих джерел переходить із аномального стану у нормалізований режим функціонування, що ускладнює детекцію інцидентів. Зокрема, сценарії компрометації із навмисним вимкненням журналювання можуть залишатися невиявленими через неможливість диференціації між технічною недоступністю та зловмисною активністю [28]. Узагальнено, масові відключення електропостачання в розподіленій ІКС призводять до розриву мережевих зв'язків і втрати частини телеметрії, що не досягає центру моніторингу та реагування. Одночасно засоби захисту, розгорнуті на відключених вузлах, припиняють виконання функцій контролю та реагування щодо відповідних активів [46][18][38][39][40]. Схематично даний феномен відображено на рис.1 [46].

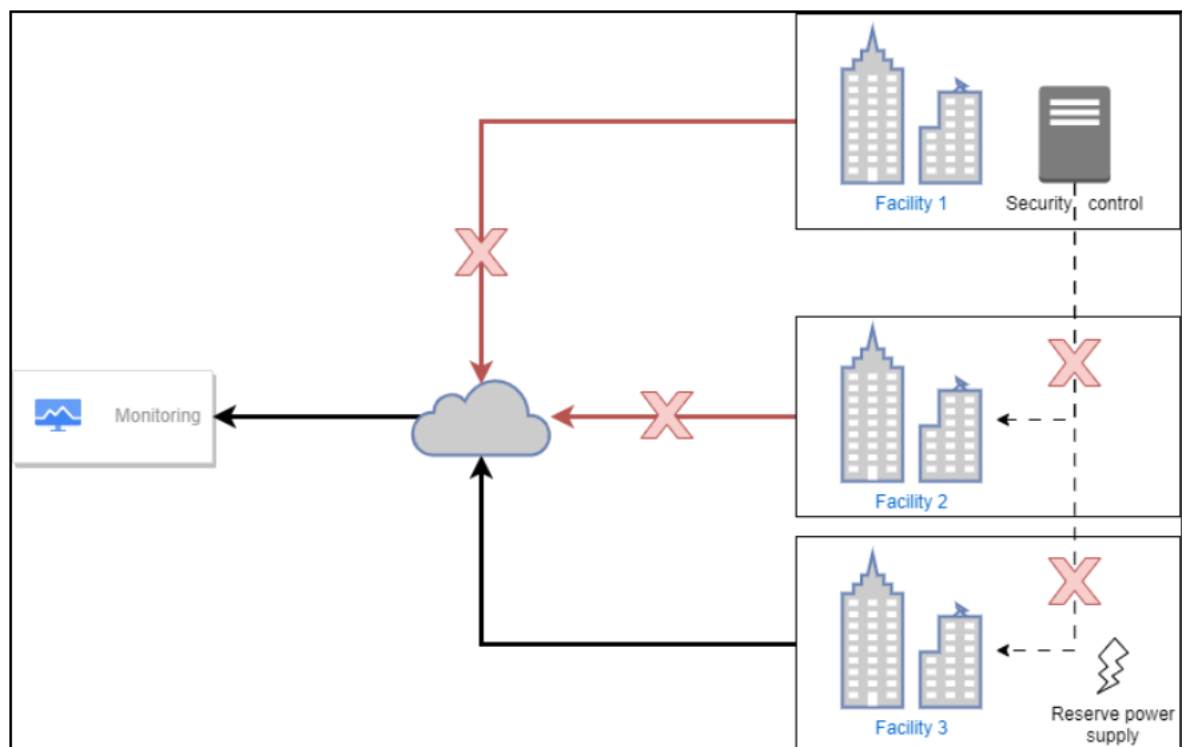


Рисунок 1 - Принципова схема, що відображає фактори впливу відключення електропостачання на кібербезпеку розподіленої ІКС [46]

Нижче наведено Таблицю 1, у якій описано різні об'єкти динамічної інфраструктури з акцентом на їхню роль у забезпеченні кібербезпеки та потенційні наслідки відключень електроенергії для цих систем.

Таблиця 1 - Динамічні об'єкти інфраструктури та їхній вплив на кібербезпеку [46]

Тип об'єкта	Опис об'єкта	Приклад використання в контексті безпеки	Можливий розширений вплив на безпеку об'єкта та пов'язаної інфраструктури в разі відключення живлення
Об'єкти з конфігурацією DHCP	Пристрої та програмне забезпечення, які отримують IP-конфігурацію від DHCP-сервера.	Автоматичне призначення IP-адрес пристроям у мережі.	Втрата IP-конфігурації під час відключення живлення може призвести до мережових збоїв, IP-конфліктів і потенційного несанкціонованого доступу до невірних призначених адрес або конфігурацій за замовчуванням. Зміни в адресному розподілі у системах Deception можуть спричинити хибні спрацювання.

			Кешовані дані DNS і IP-інформація SIEM можуть ускладнити аналіз під час інциденту.
Кеш в оперативній пам'яті	Тимчасові області зберігання в RAM, що використовуються для прискорення процесів отримання даних.	Кешування даних аутентифікації користувача для пришвидшення процесу авторизації.	Втрата кешованих даних може порушити доступність агентів аутентифікації через завершення терміну дії облікових даних, що потребуватиме взаємодії з користувачем і може вплинути на загальну доступність системи. Форензика значною мірою залежить від аналізу кешованих даних.
Волатильні конфігурації в оперативній пам'яті	Налаштування і стани, що зберігаються в RAM та не записуються у постійну пам'ять.	Зміни конфігурації під час роботи в мережеских пристроях.	Відключення живлення може призводити до втрати конфігурацій, викликаючи повернення до застарілих або стандартних налаштувань під час перезапуску. Це

			створює операційні невідповідності, порушення в безпекових протоколах і продовжує простої системи.
Динамічні маршрути	Маршрути, що змінюються в режимі реального часу відповідно до змін у мережі.	Адаптивна маршрутизація на основі трафіку та умов у мережі.	Порушення динамічної маршрутизації під час збоїв живлення може призвести до втрати або неправильної маршрутизації пакетів даних. Ефект проявляється у порушенні цілісності мережі, призводить до відмови в обслуговуванні, особливо в реальному часі.
VPN-тунелі	Захищені з'єднання, встановлені через Інтернет, що з'єднують дві мережі.	Захищений віддалений доступ до корпоративної мережі.	Відключення живлення спричиняє обрив VPN-тунелів, що потребує повторної аутентифікації та встановлення з'єднання, що значно затримує безпечну комунікацію. Також

			можливе зниження стабільності мережі.
Дані в оперативній пам'яті (RAM)	Дані, що тимчасово зберігаються в RAM під час активних сесій.	Зберігання ключів дешифрування під час сесії.	Будь-яке відключення живлення призводить до повного стирання даних у RAM, що унеможлиблює відновлення сесійно-залежних даних, таких як ключі шифрування, сеансові токени або відкриті з'єднання.

[46]

1.4. Оцінка впливу на спостережність інформації для кожного типу волатильних об'єктів

Динамічні компоненти інформаційно-комунікаційної інфраструктури залежать від стану, що формується під час роботи системи та повністю або частково зберігається в оперативній пам'яті (Random Access Memory, RAM). До цієї групи належать таблиці адресних оренд, кешовані дані, активні конфігурації, маршрути, параметри захищених з'єднань і контекст виконуваних процесів. Відключення електроживлення перериває підтримання такого стану, а після запуску система відновлюється за доступними персистентними даними, які можуть бути неповними або застарілими. Унаслідок цього операційний стан після відновлення може відрізнятися від стану перед відключенням [37][42][44][43][49].

Одним із перших проявів цієї залежності є порушення роботи протоколу динамічного конфігурування вузлів (Dynamic Host Configuration Protocol, DHCP). DHCP-сервер підтримує унікальність IP-адрес за допомогою таблиці

оренд, однак збій живлення може призвести до втрати або десинхронізації її актуального стану. Після масового запуску клієнти повторно надсилають запити DHCP Discover, тоді як сервер може використовувати застарілу чи пошкоджену базу. За таких умов одна адреса може бути видана кільком вузлам, що спричиняє конфлікти IP-адрес, помилки маршрутизації, втрату доступності сервісів і порушення цілісності передавання даних [49] [43][46]. Під час одночасного відновлення значної кількості пристроїв зміни адрес набувають хвильового характеру, відомого як DHCP churn, і затримують стабілізацію мережі [37][49] [51].

Масове перепризначення адрес також порушує зв'язок між фізичним активом і його мережевим ідентифікатором. Той самий вузол у різні моменти часу фіксується під різними IP-адресами, а одна адреса може послідовно належати різним вузлам. Журнали подій у такому разі утворюють фрагментоване представлення активності. Система управління інформацією та подіями безпеки (Security Information and Event Management, SIEM) може помилково об'єднати події різних активів або розділити події одного активу між кількома сутностями. Це ускладнює кореляцію, атрибуцію дій і відтворення послідовності інциденту [37][44][49].

Інший клас порушень пов'язаний із кешуванням даних в оперативній пам'яті. In-memory cache зменшує затримку доступу та навантаження на основні сховища, але без механізмів персистентності втрачає весь непідтверджений стан після припинення живлення. Типовим прикладом є Redis, який може використовуватися як кеш, база даних або брокер повідомлень. Втрата сесій, фрагментів контенту, аналітичних даних і незбережених змін порушує узгодженість між кешем та основним сховищем [44] [49] [46]. Після запуску починається повторне наповнення кешу, що тимчасово збільшує навантаження на серверні компоненти та погіршує продуктивність. Якщо в оперативній пам'яті зберігалися сесійні стани, оперативні журнали або транзакційні контексти засобів захисту, їх зникнення створює прогалини в телеметрії та скорочує кількість артефактів, доступних для аналізу інциденту [37][44] [49].

Подібний механізм діє для конфігурацій, що застосовуються безпосередньо з оперативної пам'яті. Після перезавантаження вони мають бути відтворені з файлів, централізованих систем керування або інших джерел. За відсутності актуальної персистентної копії система запускається зі стандартними, попередніми чи внутрішньо неузгодженими параметрами. У мережевій безпеці це стосується, зокрема, правил фільтрації iptables. Їх втрата може тимчасово змінити політики доступу та сегментації. Відновлення коректної конфігурації збільшує цільовий час відновлення (Recovery Time Objective, RTO), а до завершення цього процесу захисні механізми можуть функціонувати з ослабленими або неповними обмеженнями [37][44] [52] [49].

Динамічна маршрутизація є окремим випадком залежності від волатильного стану. Після знеструмлення маршрутизатор втрачає актуальну інформацію про суміжні вузли та обчислені маршрути. Протокол відкритого найкоротшого шляху (Open Shortest Path First, OSPF) і протокол граничного шлюзу (Border Gateway Protocol, BGP) після запуску повторно формують таблиці маршрутизації. До завершення конвергенції можливі нестійкі маршрути, цикли або «чорні діри», через які пакети втрачаються чи надходять із затримкою. Порушується доставка журналів і телеметрії, виникають розриви в сегментації, ускладнюються ізоляція вузлів, перенаправлення трафіку та застосування мережових політик під час реагування [37][44] [49].

Віртуальні приватні мережі (Virtual Private Network, VPN) залежать як від доступності кінцевих шлюзів, так і від стану проміжної мережевої інфраструктури. Відключення живлення розриває тунелі між майданчиками та припиняє роботу захищених каналів. За наявності автоматичного резервного маршруту трафік може бути спрямований через канал, для якого не забезпечено еквівалентний рівень шифрування і контролю, що створює передумови для перехоплення або атаки посередника [44][45][49] [53]. У конфігураціях, де VPN одночасно забезпечує сегментацію та проходження трафіку через міжмережіві екрани або системи виявлення вторгнень, відмова тунелю змінює фактичну схему застосування контролів. Віддалений сегмент може стати недоступним для моніторингу або перейти на маршрут із неповним покриттям засобами захисту.

Для команди реагування це означає втрату керованого доступу до активів і затримку операцій локалізації [37][44] [49].

Окремі втрати виникають на рівні даних, що існують лише в RAM. Стан процесів, активні мережеві з'єднання, сеанси користувачів, відкриті дескриптори, незбережені ключі та інші контекстні відомості використовуються для цифрового криміналістичного дослідження. Після знеструмлення ці дані не можуть бути вилучені звичайними засобами, тому часову послідовність інциденту доводиться відновлювати за дисковими артефактами та мережевими журналами, які містять менше відомостей про стан системи в момент компрометації [44] [49]. Особливо суттєвою є втрата ознак шкідливого програмного забезпечення, резидентного в пам'яті, а також відомостей про активні сесії та з'єднання [37][44][51][49].

1.5. Технології та методи протидії впливам деградації інфраструктури на спостережність інформації

Більшість політик безпеки інформаційно-комунікаційних систем (ІКС) враховують відключення електроживлення як обмежений за тривалістю інцидент і передбачають відповідні контрзаходи (резервування, відновлення, деградаційні режими) [47] [48] [49] [50]. Проте ці моделі не охоплюють сценарії систематичного руйнування енергетичної інфраструктури, яке має зовнішній характер і не контролюється на рівні ІКС [46].

У таких умовах відключення набувають масового, повторюваного та тривалого характеру. Емпірично зафіксовано, що під час енергетичного дефіциту середня тривалість відключень у місті Київ становила близько 4 годин до трьох разів на добу, з піковими значеннями до 72 годин у межах окремих районів під час масштабних відключень електропостачання. Такі параметри суттєво перевищують припущення, закладені у класичних моделях відмов. Неврахування подібних режимів призводить до некоректної оцінки ризиків і відсутності адекватних контрзаходів у моделях загроз. У подальшому доцільно розглянути типові механізми забезпечення стійкості ІКС до відключень

електроживлення та їх обмеження в умовах довготривалих і повторюваних збоїв [54].

1.5.1. Резервування каналів зв'язку

Під час масштабних відключень електропостачання використання однотипних каналів зв'язку може бути ризикованим, в особливості якщо цей тип каналу є енергозалежним на останній ділянці від провайдера — як, наприклад, UTP/FTP, коаксіальний кабель, тощо. Дані типи каналів зв'язку передбачають наявність у провайдера обладнання щодо резервування електроживлення, що створює додаткові ризики відключень [46].

1.5.2. Резервування електроживлення.

Батареї резервного живлення (Uninterruptible Power Supply, UPS) забезпечують підтримку працездатності обладнання протягом обмеженого часу після втрати централізованого електроживлення. Ефективність такого підходу обмежується ємністю акумуляторів: для забезпечення тривалої роботи серверної інфраструктури необхідні системи великої енергоємності, що супроводжується значними капітальними витратами [56] [59]. Додатково, експлуатація в режимі глибоких циклів розряду прискорює деградацію акумуляторів і зменшує їх ресурс, що підвищує операційні витрати на заміну. В умовах масових і регулярних відключень виникає ще одне обмеження: тривалість повного заряду може перевищувати доступний інтервал між відключеннями, внаслідок чого батареї не відновлюють номінальну ємність. Це призводить до кумулятивного зниження ефективності резервування та втрати гарантій безперервності функціонування [46].

Генераторні установки є найбільш ефективним засобом резервного електроживлення ІКС, оскільки тривалість їх автономної роботи визначається моторесурсом та обсягом доступного палива [54][56]. На відміну від акумуляторних систем, вони здатні підтримувати функціонування інфраструктури протягом тривалих періодів. Водночас їх застосування обмежується інфраструктурними та організаційними факторами: необхідність виділення спеціалізованих приміщень, дотримання технічних умов

експлуатації, а також значні капітальні витрати. Для географічно розподілених ІКС масштабування такого підходу ускладнюється логістикою постачання палива та координацією обслуговування, що підвищує загальну вартість і складність забезпечення безперервності [46] [60].

1.5.4. Географічне розподілення ІКС.

Географічний розподіл об'єктів ІКС використовується як механізм диверсифікації ризиків відмов електроживлення з огляду на ефективність підходу для однорідних компонентів, де часткова деградація не призводить до повної зупинки системи. Водночас для критичних міжзалежних компонентів різного класу відмова одного вузла може спричинити повну втрату функціональності, що обмежує ефективність розподілу. У випадку масштабних або синхронізованих відключень на рівні країни географічна диверсифікація в межах однієї енергосистеми втрачає ефективність. Натомість міждержавний розподіл, особливо між енергетично незалежними регіонами, дозволяє суттєво знизити ризики, пов'язані з відмовами електроживлення [46].

1.5.5. Розподілення ІКС з використанням потужностей хмарних провайдерів.

Використання хмарних сервісів є ефективним механізмом диверсифікації ризиків відмов електроживлення для окремих компонентів ІКС. Провайдери глобального масштабу (Amazon, Google, Microsoft) забезпечують високу стійкість інфраструктури за рахунок географічного розподілу та багаторівневого резервування живлення, що мінімізує вплив локальних енергетичних збоїв. Винесення окремих сервісів у хмару дозволяє ізолювати їх від локальних відключень і забезпечити безперервність функціонування, зокрема для компонентів класу WAF, SIEM та EDR. Водночас повна міграція ІКС є неможливою через залежність від локальних активів (робочі станції, внутрішні сервіси) та засобів захисту мережевого рівня (міжмережеві екрани, IPS; IDS) [55] [46].

Критичним обмеженням є залежність від каналів зв'язку: доступ до хмарних ресурсів потребує стабільного високошвидкісного з'єднання. В умовах

енергетичних збоїв доступні альтернативи (супутниковий зв'язок ≈ 100 Мбіт/с; ADSL до ≈ 27 Мбіт/с) не забезпечують достатньої пропускної здатності для повноцінного функціонування середніх і великих ІКС. Хмарна диверсифікація знижує ризики відключень електроживлення лише частково та потребує врахування обмежень мережевої доступності [46] [53-57].

1.6. Порівняльний аналіз технологій та методів протидії впливам відключень електропостачання

Розглядаючи наявні проблеми кібербезпеки, пов'язані з масовими відключеннями електропостачання, в поєднанні з існуючими контрзаходами щодо протидії періодичним відключенням, можна зробити висновки щодо того, які заходи можуть бути ефективні в нівелюванні ризиків саме в розглянутій ситуації. Короткі результати порівняльного аналізу наводяться в таблиці 2.

Таблиця 2 - порівняльний аналіз заходів протидії впливу відключень електропостачання [46]

Контрзахід	Переваги	Недоліки
Резервне живлення від батарей (ДБЖ)	Забезпечення функціонування об'єкту в умовах відключення електропостачання; Можливість моніторингу стану батареї, що зменшує ризики щодо спостережності.	Час підтримки функціонування об'єкту відносно нетривалий; Потребує істотних фінансових вкладень для забезпечення усіх об'єктів, особливо стосовно серверного обладнання.
Резервні генератори	Забезпечення функціонування об'єкту в умовах відключення	Потребує істотних фінансових вкладень для забезпечення усіх об'єктів ІКС;

	електропостачання протягом потенційно необмеженого часу; Можливість резервування порівняльно більшої електричної потужності.	Створює логістичне та організаційне навантаження на підтримку функціонування; Ускладнений централізований моніторинг стану генераторів.
Географічне розподілення	Можливість нівелювати ризики відключень по відношенню до однотипних компонентів системи; У разі міждержавного розподілу дозволяє забезпечити гарантований захист частини ІКС.	Не вирішує проблему відключення унікальних компонентів ІКС; Не забезпечує захисту від загальнодержавних відключень.
Перенесення в хмару	Гарантований захист від відключень електропостачання винесених компонентів.	Неможливо перенести усі компоненти ІКС в хмару.

1.7. Оцінка ефективності існуючих підходів до протидії втраті спостережності в умовах деградації інфраструктури

1.7.1. Обмеження інфраструктурних методів підтримки спостережності

Розглянуті методи резервування електроживлення, каналів зв'язку, географічного розподілення компонентів та використання хмарних

обчислювальних ресурсів зменшують імовірність повної зупинки окремих елементів інформаційно-комунікаційної системи. Водночас ці методи не забезпечують збереження спостережності як властивості всієї системи управління подіями безпеки. Їх основним об'єктом є фізична або мережева доступність компонентів, тоді як спостережність залежить від повноти, своєчасності, узгодженості та достовірності телеметрії, актуальності відомостей про активи й можливості встановлення зв'язків між подіями.

Резервне електроживлення підтримує роботу обладнання лише протягом часу, визначеного ємністю акумуляторів, запасом палива, режимом навантаження та доступністю технічного обслуговування. Часткове резервування не гарантує одночасної доступності всього ланцюга формування телеметрії. Джерело подій може продовжувати роботу, тоді як окремі центральні чи проміжні частини системи залишатимуться недоступними. Збереження працездатності одного компонента за відмови іншого не усуває розрив потоку подій і не забезпечує можливості відновити втрачений контекст. Перехід між основним і резервним живленням також не вирішує проблематику втрати спостережності. Події характерні для втрати електроживлення, які зовні можуть відповідати ознакам порушення доступності, зміни конфігурації, вимкнення засобу захисту або втручання в мережеву інфраструктуру. Резервування зменшує тривалість фізичної відмови, але не усуває невизначеність щодо причин подій, сформованих під час деградації та відновлення.

Резервування каналів зв'язку обмежується наявністю спільних точок відмови. Основний і резервний канали можуть залежати від одного енергетичного вузла, провайдера, кабельної траси або майданчика. Після переходу на альтернативне з'єднання змінюються пропускна здатність, затримка, порядок доставлення пакетів і фактичний маршрут передавання телеметрії. За недостатньої пропускної здатності пріоритет може надаватися прикладному трафіку, тоді як передавання журналів затримується або припиняється. Центральна система продовжує функціонувати, але її інформаційний стан уже не відповідає фактичному стану віддаленої

інфраструктури, тобто проблематика погіршення спостерожності може не лише не вирішитись, але й зазнати певного погіршення.

Географічне розподілення знижує ризик одночасної відмови лише за умови незалежності майданчиків і взаємозамінності розміщених на них компонентів. Для унікальних джерел даних, систем ідентифікації, мережевих шлюзів або технологічних сегментів перенесення функцій на інший майданчик може бути неможливим. У випадку масштабних впливів у межах однієї енергетичної або телекомунікаційної системи географічна віддаленість не означає незалежності відмов. Додатково розподілення збільшує кількість мережевих залежностей і варіантів маршрутизації, через що ускладнюється визначення фактичного стану активів. Перенесення центральних компонентів до хмарного середовища забезпечує доступність сховища, аналітичної платформи або консолі керування, однак не забезпечує безперервного формування й доставлення телеметрії від локальних активів. Хмарна система управління інформацією та подіями безпеки може залишатися працездатною за одночасної втрати даних від значної частини контрольованої інфраструктури. За таких умов доступність центральної платформи не є достатнім показником доступності функції моніторингу. Аналогічне обмеження стосується хмарних засобів керування кінцевими точками: агент може продовжувати локальну роботу, але бути недоступним для централізованого аналізу та реагування через втрату каналу зв'язку.

Існуючі методи резервування спрямовані переважно на зниження тривалості простою та відновлення функціонування компонентів. Вони не містять засобів формального оцінювання ступеня втрати спостережності, не визначають довіру до даних після відновлення та не забезпечують автоматичної диференціації між інфраструктурною деградацією і діями загрозового агента. У результаті інформаційна система може залишатися частково працездатною, але формувати неповне або помилкове представлення стану контрольованої інфраструктури.

1.7.2. Вплив втрати спостережності на збір і попередню обробку телеметрії

Методи збору та попередньої обробки ґрунтуються на припущенні, що джерело подій, канал передавання і колектор доступні з достатньою регулярністю, а часові мітки й ідентифікатори джерел залишаються узгодженими. Руйнування енергетичної та телекомунікаційної інфраструктури порушує кожне з цих припущень.

Переривання зв'язку призводить до втрати подій або їх відкладеного надходження після відновлення каналу. Якщо джерело підтримує локальну буферизацію, події можуть бути передані пакетом із затримкою. Центральна система отримує записи, час виникнення яких істотно відрізняється від часу надходження. Якщо аналітичний конвеєр не розрізняє ці часові характеристики, події можуть бути включені до неправильного інтервалу аналізу або оброблені після завершення відповідного кореляційного вікна.

Повторне передавання накопиченої телеметрії створює пікове навантаження на колектори та аналітичні підсистеми. Частина повідомлень може дублюватися внаслідок повторних спроб доставлення або паралельної роботи основного й резервного каналу. Дедуплікація ускладнюється, якщо після перезапуску джерела змінилися його сеансові ідентифікатори, лічильники повідомлень або часові параметри.

Аварійне вимкнення вузлів порушує синхронізацію часу. Після запуску окремі системи можуть певний період використовувати локальний годинник, який не відповідає централізованому джерелу часу. Унаслідок цього фактично послідовні події отримують суперечливі часові мітки. Помилки впорядкування поширюються на наступні етапи обробки, оскільки коректність часової кореляції та реконструкції інциденту залежить від правильного визначення порядку дій.

Фільтрація й агрегація під час масової деградації також втрачають початкову ефективність. Велика кількість однотипних повідомлень про недоступність, втрату з'єднання, завершення роботи агентів і повторну

автентифікацію може бути агрегована як один технічний стан. Проте серед цих подій можуть бути присутні окремі зловмисні дії, навмисно виконані одночасно з інфраструктурною відмовою.

1.7.3. Вплив на детерміновані методи виявлення

Детерміновані правила залежать від наявності визначених атрибутів і послідовності подій. За неповної телеметрії умова правила може не виконатися не через відсутність зловмисної активності, а через втрату одного з необхідних спостережень, що збільшує кількість хибнонегативних результатів. Сигнатурне зіставлення залишається функціональним лише для отриманих подій. Якщо журнал, мережевий потік або телеметрія кінцевої точки не були доставлені, сигнатура не має об'єкта для перевірки. Резервування центральної SIEM не компенсує відсутність даних від джерела. Порогові правила зазнають протилежного впливу. Масове завершення роботи вузлів, повторні спроби автентифікації, перепідключення агентів, зміни адрес і відновлення мережевих тунелів створюють кількісні відхилення, подібні до сканування, перебору облікових даних, мережевої атаки або масової зміни конфігурацій. Унаслідок цього збільшується кількість хибнопозитивних спрацювань.

Логічні правила з кількома умовами можуть формувати обидва типи помилок. Втрата однієї події перериває логічний ланцюг і спричиняє пропуск інциденту. Водночас поєднання технічних подій відновлення може випадково задовольнити умови правила, призначеного для виявлення зловмисної послідовності. У стабільному середовищі ці події є рідкісними, тоді як під час масової деградації вони виникають одночасно на багатьох активах. Існуючі детерміновані правила переважно не враховують підтверджений контекст втрати живлення, стан резервування, географічну приналежність активу та характер відновлення його конфігурації. Статичне зменшення чутливості правил на період відключень знижує кількість хибних спрацювань, але одночасно створює часовий інтервал зменшеного покриття, який може бути використаний для маскуванню атаки.

1.7.4. Вплив на комплексну обробку та кореляцію подій

Комплексна обробка подій передбачає збереження стану, контроль часових вікон і встановлення послідовності між простими подіями. Відкладене доставлення, зміна порядку повідомлень і повна відсутність окремих елементів послідовності порушують формальні умови СЕР-шаблонів. Подія, яка надійшла після завершення встановленого часового вікна, може бути відкинута як нерелевантна, хоча фактично вона належить до відповідного сценарію. Збільшення вікна частково компенсує затримку, але підвищує ймовірність випадкового об'єднання незалежних подій. В умовах непередбачуваної тривалості відключень неможливо визначити універсальний часовий інтервал, який одночасно забезпечував би повноту та прийнятну точність.

Виявлення відсутності очікуваної події також стає неоднозначним. Припинення контрольних повідомлень може означати вимкнення агента зловмисником, фізичне знеструмлення вузла, розрив каналу, перевантаження колектора або затримку доставлення. Без додаткового контексту СЕР фіксує лише факт відсутності, але не встановлює його причину. Атрибутивна кореляція погіршується через несталість ідентифікаторів. Зміна IP-адрес, повторна реєстрація агента, формування нового сеансу або відновлення вузла з попередньої конфігурації призводять до розділення подій одного активу. Водночас повторне використання адреси може спричинити об'єднання активності різних активів.

Часова кореляція порушується через розбіжності годинників і затримки передавання. Просторова кореляція залежить від актуальної інформації про належність активу до сегмента або майданчика, однак під час аварійної маршрутизації фактичний шлях телеметрії та логічна топологія можуть змінюватися.

Кореляція на основі передумов і наслідків є особливо чутливою до пропусків. Якщо подія, яка підтверджує досягнення проміжного стану, втрачена, наступна подія не може бути формально пов'язана з попередньою. Система або відкидає коректний сценарій, або змушена формувати припущення

щодо відсутніх етапів. У першому випадку збільшується кількість хибнонегативних висновків, у другому — кількість непідтверджених гіпотез, які потребують перевірки аналітиком.

1.7.5. Вплив на кластеризацію, статистичний і поведінковий аналіз

Методи кластеризації в період деградації отримують масив подій, структура якого визначається не поведінкою загрозового агента, а спільною інфраструктурною причиною. Події недоступності, повторного запуску, зміни мережевих параметрів і відновлення агентів утворюють великі однорідні кластери. Такі кластери можуть витіснити з аналізу менші групи зловмисної активності або об'єднувати їх із технічними відмовами. Аналіз першопричин за статистичною подібністю в такому середовищі визначає відключення електроживлення або каналу як домінуючу причину. Цей результат є формально коректним для більшості подій, але не дозволяє встановити, чи присутня в межах кластера окрема атака. Для виявлення зловмисного накладання необхідні ознаки, які відображають відхилення конкретного активу від загального профілю деградації. Статистичні методи виходять із наявності відносно сталого розподілу нормальної активності. Масові відключення та хвилі відновлення змінюють середні значення, дисперсію, сезонність і частоту подій. Сформована раніше модель починає класифікувати значну частину легітимної активності як аномальну.

Для поведінкового аналізу виникає проблема зміни контексту. Після відновлення актив може отримати нову адресу, сформувати новий профіль мережевих зв'язків або працювати через альтернативний маршрут. Алгоритм може інтерпретувати це як поведінку нового об'єкта або як істотне відхилення від попередньої моделі. В обох випадках результат визначається інфраструктурною перебудовою, а не станом кібербезпеки.

1.7.6. Вплив на причинно-наслідні та графові методи

Причинно-наслідні та графові методи залежать від актуального представлення активів, їхніх ідентичностей, мережевих зв'язків і

функціональних залежностей. Деградація інфраструктури змінює ці відношення швидше, ніж вони відображаються в централізованих реєстрах.

Після аварійної зміни маршруту фактичний шлях між вузлами може не відповідати графу мережевої доступності. Після втрати активу або сегмента в графі залишаються вершини й ребра, які більше не є функціональними. Після відновлення з новими ідентифікаторами один фізичний об'єкт може бути представлений кількома вершинами. За неповної телеметрії граф атаки містить розриви. Алгоритм не може визначити, чи відсутній перехід не відбувся, чи лише не був зафіксований. Формування гіпотетичних ребер дозволяє продовжити реконструкцію, але зменшує доказовість результату. Кількість можливих шляхів збільшується, а вибір між ними потребує додаткових даних, які під час деградації можуть бути недоступними.

Помилкова топологія впливає також на прогнозування поширення атаки та вибір заходів локалізації. Рекомендована ізоляція вузла може бути технічно нездійсненною через недоступність засобу керування або спричинити відмову залежних сервісів, зв'язки з якими не відображені в актуальній моделі.

1.7.7. Вплив на контекстне збагачення, оцінювання ризику та ретроспективний аналіз

Контекстне збагачення підвищує точність аналізу лише за умови актуальності приєднаних відомостей. Під час деградації змінюються статус активу, його мережеві ідентифікатори, фактичний майданчик, доступність засобів захисту та керованість. Централізований реєстр може зберігати попередній стан і використовувати його для збагачення нових подій.

Помилковий контекст має системний характер. Якщо події приєднуються до неправильного активу, подальша кореляція, оцінювання критичності й пріоритезація також стають некоректними. Висока критичність помилково визначеного активу підвищує пріоритет технічного оповіщення, тоді як реальна подія на іншому вузлі може отримати занижену оцінку.

Методи оцінювання ризику зазвичай враховують серйозність сигналу, критичність активу, релевантність загрози та впевненість у результаті. В умовах втрати спостережності невизначеність вхідних даних збільшується, але не завжди включається до функції ризику. У результаті числова оцінка створює формальне враження точності, хоча частина її параметрів ґрунтується на застарілих або неповних відомостях.

Ретроспективний аналіз безпосередньо залежить від повноти журналів і збереження волатильних даних. Аварійне вимкнення знищує інформацію про активні процеси, мережеві з'єднання, сеанси, незбережені ключі й об'єкти, резидентні в оперативній пам'яті. Перерви журналювання створюють часові інтервали, для яких неможливо підтвердити або спростувати гіпотезу щодо дій агента загроз.

Зміна адрес, розбіжності часових міток і повторна реєстрація компонентів ускладнюють побудову єдиної часової шкали. Встановлення початкової точки компрометації, тривалості присутності та переліку заторкнутих активів потребує додаткових припущень.

1.7.8. Невирішені аспекти протидії втраті спостережності

Результати аналізу не дозволяють вважати існуючі підходи достатніми для підтримки процесів управління подіями безпеки в умовах систематичної деградації інфраструктури. Резервування та розподілення знижують імовірність повної відмови окремих компонентів, але не забезпечують цілісного й достовірного представлення стану ІКС за часткової недоступності джерел даних.

У наявних підходах відсутній єдиний механізм, який одночасно:

- визначає факт і ступінь втрати спостережності;
- враховує стан живлення, зв'язку, джерел телеметрії та засобів реагування;
- підтримує актуальне відображення подій на активи за зміни їхніх ідентифікаторів;

- відрізняє масову інфраструктурну деградацію від вибіркової зловмисної активності;
- модифікує правила кореляції та пріоритезації відповідно до якості доступних даних;
- зберігає походження, час підтвердження та рівень довіри до контекстних атрибутів;
- надає аналітику формалізовану оцінку невизначеності результату.

Проведений аналіз показав що задача повного усунення впливів військового часу на спостережність інформації в комп'ютерній системі управління подіями не вирішена, що зумовлює стан невизначеності та ряд негативних впливів на операційні функції комп'ютерної системи управління подіями безпеки. Визначення цих впливів, та розробка методів протидії даним впливами є актуальною науковою задачею.

Висновки

У розділі ідентифіковано існуючі методи обробки та аналізу подій безпеки в комп'ютерних системах управління подіями. Завдання вирішено шляхом систематизації методів за послідовними рівнями перетворення інформації: збору та попередньої обробки телеметрії; детермінованого виявлення визначених ознак; комплексної обробки подій; агрегації та кореляції оповіщень; кластеризації та аналізу першопричин; статистичного і поведінкового аналізу; причинно-наслідкового та графового моделювання; контекстного збагачення; оцінювання ризику; ретроспективного аналізу та реконструкції інцидентів. Встановлено, що коректність застосування цих методів залежить від повноти, своєчасності, достовірності й узгодженості телеметрії, сталості ідентифікаторів активів, актуальності топологічної та інвентаризаційної інформації. Сигнатурні й детерміновані методи залежать від наявності визначених атрибутів; комплексна обробка та кореляція - від збереження часових і причинних зв'язків; статистичні методи - від стабільності моделі нормального стану; графові й контекстні методи - від актуальності даних про активи та їхні залежності.

У розділі визначено ключові фактори впливу повномасштабної війни на процеси обробки та аналізу подій у комп'ютерних системах управління подіями безпеки. Завдання вирішено шляхом систематизації специфічних для воєнного часу чинників, що змінюють умови збору, доставлення, нормалізації та інтерпретації телеметрії: руйнування енергетичної та телекомунікаційної інфраструктури; окупація і фізична втрата об'єктів інформаційно-комунікаційних систем; кадрова криза; інтенсифікація кібервійни; вимушена хмарна міграція і географічне перерозподілення інфраструктурних об'єктів. В ході виконання завдання було відображено прямий вплив даних факторів на параметри спостережності інформації в комп'ютерних системах управління подіями безпеки. Швидка деградація електроживлення, каналів зв'язку та фізичної доступності активів спричиняє фрагментацію моніторингу, ізоляцію сегментів, втрату зв'язку із сенсорами, затримку доставлення журналів, знищення волатильних даних і змішування ознак технічної недоступності компонентів з можливою активністю агента загроз.

У розділі оцінено ефективність існуючих підходів до протидії втраті спостережності в умовах деградації інфраструктури та інших специфічних факторів воєнного часу. Завдання вирішено шляхом порівняльного аналізу існуючих підходів, а саме резервування електроживлення за рахунок джерел безперебійного живлення та генераторів, резервування каналів зв'язку, географічного розподілення інформаційно-комунікаційних систем, використання потужностей хмарних провайдерів і моніторингу стану електроживлення, зв'язку та джерел журналювання. Встановлено, що ці підходи зменшують окремі ризики фізичної та мережевої доступності, але не забезпечують усунення проблеми втрати спостережності всієї системи, особливо в контексті географічної розподіленості. Отриманий результат засвідчує необхідність розроблення методів, які враховують неповноту телеметрії, змінність інфраструктури та невизначеність причин втрати спостережності.

За результатом проведеного аналізу зроблено висновок про недостатність суто інфраструктурних контрзаходів в розрізі протидії втраті спостережності

інформації і необхідність розробки методів зменшення чи повного усунення негативного впливу погіршення спостережності ІКС у військових умовах на процеси моніторингу, обробки та аналізу подій безпеки.

РОЗДІЛ 2. РОЗРОБКА МЕТОДІВ ТА АЛГОРИТМІВ ПОКРАЩЕННЯ СПОСТЕРЕЖНОСТІ ІНФОРМАЦІЇ

2.1. Визначення метрик оцінки впливу втрати спостережності та специфічних військових факторів на операційні процеси обробки подій кібербезпеки

У попередньому підрозділі визначено фактори повномасштабної війни, які порушують роботу комп'ютерних систем управління подіями безпеки: деградацію електроживлення і каналів зв'язку, фізичну втрату або переміщення активів, інтенсивні топологічні зміни, кадрові обмеження та зростання кількості атакуючих впливів. Спільним наслідком цих факторів є зменшення обсягу інформації про фактичний стан інфраструктури, збільшення затримок доставлення телеметрії та порушення зв'язку між подіями й активами [49].

2.1.1. Причинно-наслідне представлення впливу

Вплив воєнного середовища подається послідовністю «фактор порушення - втрата спостережності або керованості - зміна операційної метрики». Деградація електроживлення вимикає активи, сенсори, колектори та мережеві вузли. Порушення каналів зв'язку перериває або затримує доставлення журналів. Фізична втрата контролю над майданчиком знижує довіру до даних, що надходять із нього. Топологічні зміни ускладнюють коректне відображення подій на активи. Кадровий дефіцит зменшує пропускну здатність аналітичних процесів. Зростання інтенсивності атак збільшує фактичну кількість інцидентів та одночасне навантаження на SOC. Для опису зазначених впливів достатньо виділити три проміжні стани: втрату спостережності, збільшення аналітичного навантаження та зниження доступності засобів реагування. Втрата спостережності визначає повноту і достовірність вхідних даних. Аналітичне навантаження залежить від кількості інцидентів, технічних аномалій і хибнопозитивних спрацювань. Доступність реагування характеризує можливість виконати ізоляцію активу, блокування взаємодії, зміну конфігурації або іншу керовану дію.

Як аналітичну рамку використано модель зрілості спроможностей операційного центру кібербезпеки (SOC Capability Maturity Model, SOC-CMM), яка містить показники ресурсного забезпечення, доступності технологічної платформи, якості виявлення та часових характеристик реагування [58]. До кількісної частини моделі включено лише показники, безпосередньо пов'язані зі спостережністю та циклом «виявлення — аналіз — реагування». Інші показники збережено як якісні характеристики загального операційного стану SOC.

Таблиця 3 - очікуваний вплив воєнних факторів на групи операційних метрик SOC [49][58]

Група	Метрики SOC-CMM	Напрямок зміни
Ресурсне забезпечення	Budget spent vs budget forecasted; кількість відкритих вакансій; Recruitment time; Turnover rate; Retention time; Overbooked time	Витрати, вакансії, строки найму, плинність і перевантаження зростають; строк утримання скорочується
Спостережність і технологічна доступність	MITRE ATT&CK visibility (data sources); Availability of SOC technology (uptime); Log source downtime	Покриття і доступність зменшуються; простій джерел зростає
Якість виявлення	Percentage of false positives; Number of false negatives; Alerts not analysed	Зростання
Часові показники	Mean time to pick-up; Mean time to analyse; Mean time to detect; Mean time to respond; Mean time to contain; Average time to resolve vulnerabilities	Збільшення

Група	Метрики SOC-CMM	Напрямок зміни
Інциденти та вразливості	Mean time between incidents; Number of incidents; Number of high and critical overdue vulnerabilities	Інтервал між інцидентами і скорочується; кількість інцидентів і прострочених вразливостей зростає

Показники бюджету, найму, утримання персоналу та накопичення вразливостей не включаються до основного вектора моделі. Вони залежать від організаційних і фінансових рішень, тому використовуються для пояснення загального стану SOC, але не для безпосереднього обчислення втрати спостережності.

2.1.2. Метрика втрати спостережності

Спостережність у межах дослідження визначається як здатність системи отримувати достатні, своєчасні та достовірні дані для встановлення стану активів, виявлення інцидентів і обґрунтування дій реагування. Втрата спостережності виникає не лише за повної недоступності джерела. Вона також охоплює затримку доставлення журналів, втрату окремих фрагментів телеметрії, невизначене походження даних і помилкове відображення події на актив.

Нехай система використовує n джерел спостереження. Для кожного джерела i задається вага w_i , яка характеризує його значення для контролю інфраструктури, та часткова втрата $l_i(t)$ у діапазоні від 0 до 1. Значення 0 відповідає нормальній роботі джерела, 1 — повній непридатності його даних. Проміжні значення відображають неповноту, затримку або зниження довіри. Інтегральна метрика втрати спостережності визначається як зважена частка втрат:

$$Lobs(t) = \sum w_i l_i(t) / \sum w_i, \quad 0 \leq Lobs(t) \leq 1 \quad (2.1)$$

Значення $Lobs(t)$, близьке до нуля, характеризує стан, у якому необхідна телеметрія доступна та придатна до використання. Зростання показника означає збільшення частки інфраструктури або класів подій, стан яких не може бути надійно встановлений. Ваги дозволяють відрізнати втрату другорядного джерела від недоступності сенсора, що забезпечує спостереження критичного сегмента або унікального класу атак.

Для оцінювання саме додаткового воєнного впливу значення $Lobs(t)$ порівнюється з базовим рівнем $Lobs_0$, визначеним за стабільний період. Позитивна різниця між поточним і базовим значеннями характеризує приріст втрати спостережності. Такий підхід не дозволяє віднести до наслідків війни постійні прогалини моніторингу, які існували до досліджуваного періоду.

Деградація електроживлення переважно збільшує $l_i(t)$ через вимкнення сенсорів, колекторів і мережевого обладнання. Порушення зв'язку спричиняє недоступність або затримку даних. Втрата фізичного контролю знижує довіру до джерела. Аварійна міграція, зміна адресації та маршрутів збільшують імовірність неправильного зіставлення подій з активами. Таким чином, різномірні фактори середовища зводяться до одного порівнюваного показника.

2.1.3. Вплив на інцидентність і якість виявлення

У моделі розрізняються фактична кількість інцидентів та кількість інцидентів, виявлених SOC. Це розмежування є принциповим: за високої втрати спостережності кількість зареєстрованих інцидентів може зменшитися не через покращення стану безпеки, а через збільшення кількості невиявлених подій.

Для визначеного часового інтервалу фактична кількість інцидентів NI залежить від базового рівня NI_0 , інтенсивності атак A та втрати спостережності. Інтенсивність атак збільшує кількість реальних порушень, а втрата спостережності створює додаткові можливості для розвитку інцидентів без своєчасного стримування. Спрощена залежність має вигляд:

$$NI = NI_0 \cdot (1 + k_A \cdot A + k_L \cdot Lobs) \quad (2.2)$$

Коефіцієнти kA і kL визначають чутливість конкретної інфраструктури до інтенсивності атак та зниження спостережності. Вони встановлюються за ретроспективними або експериментальними даними. Формула не використовується для прогнозування конкретної атаки, а задає очікуваний напрям зміни інцидентності.

Хибнопозитивне спрацювання (False Positive, FP) виникає, коли легітимна технічна подія класифікується як ознака інциденту. Під час відключень і відновлення інфраструктури масово виникають розриви журналювання, недоступність вузлів, перезапуски, зміни мережевих адрес і конфігурацій. За відсутності контексту такі події відповідають умовам детектування атак. Хибнонегативний результат (False Negative, FN) означає, що фактичний інцидент не був виявлений. Зростання $Lobs$ одночасно збільшує обидва типи помилок: FP — через невизначеність причин технічних аномалій, FN — через втрату доказових подій.

У спрощеній моделі ці залежності подаються лінійно:

$$FP = FP0 + b1 \cdot Lobs + b2 \cdot D; \quad FN = FN0 + c1 \cdot Lobs + c2 \cdot A \quad (2.3)$$

Тут D є нормованою інтенсивністю технічних подій деградації та відновлення, а $FP0$ і $FN0$ — базові значення. Залежності є загрубленими, але відображають основні механізми: масова інфраструктурна аномалія збільшує потік хибних сигналів, а неповна телеметрія та зростання атак — кількість пропущених інцидентів.

Для нормованої оцінки якості використовуються *Accuracy* і *Recall*. *Accuracy* характеризує частку правильних рішень серед усіх класифікованих випадків. *Recall*, або повнота виявлення, визначає частку фактичних інцидентів, які були виявлені:

$$Accuracy = (TP + TN) / (TP + TN + FP + FN); \quad Recall = TP / (TP + FN) \quad (2.4)$$

де TP — істиннопозитивні, TN — істиннонегативні результати. У термінах SOC-CMM показник *Percentage of false positives* безпосередньо пов'язаний із FP, а *Number of false negatives* — із FN. Зменшення доступності

джерел даних, відображене показником MITRE ATT&CK visibility, збільшує Lobs, знижує Recall і зазвичай зменшує Accuracy. Водночас Accuracy слід аналізувати разом із Recall, оскільки за значної переваги легітимних подій високе значення Accuracy може зберігатися навіть за неприйнятною кількістю пропущених інцидентів.

2.1.4. Вплив на MTDD і MTTR

Середній час виявлення (Mean Time to Detect, MTDD) визначається як середній інтервал між початком інциденту та його виявленням. Середній час реагування або відновлення (Mean Time to Respond/Recover, MTTR) визначається як середній інтервал від виявлення інциденту до досягнення встановленого завершального стану: стримування, відновлення сервісу або закриття інциденту. Межі вимірювання повинні бути однаковими для всіх порівнюваних періодів.

Втрата спостережності збільшує MTDD, оскільки доказова подія може не надійти, надійти із затримкою або не бути пов'язаною з потрібним активом. Додаткове аналітичне навантаження Q збільшує час очікування та аналізу. Спрощена залежність визначається як:

$$MTDD = MTDD_0 \cdot (1 + a_1 \cdot Lobs + a_2 \cdot Q) \quad (2.5)$$

MTTR залежить від тих самих факторів, а також від доступності засобів реагування R . Значення R у діапазоні від 0 до 1 характеризує ступінь втрати можливості виконувати віддалені або локальні дії. За $R = 0$ засоби реагування доступні, за $R = 1$ необхідна дія технічно неможлива або істотно обмежена:

$$MTTR = MTTR_0 \cdot (1 + d_1 \cdot Lobs + d_2 \cdot Q + d_3 \cdot R) \quad (2.6)$$

Показники $MTDD_0$ і $MTTR_0$ є базовими значеннями для стабільного періоду. Коефіцієнти a_1 , a_2 , d_1 , d_2 і d_3 визначаються для конкретного SOC. Наведені залежності не потребують моделювання черги оповіщень або окремих доменів керованості, але зберігають змістовне розмежування причин часової деградації: нестача даних, перевантаження аналітиків і недоступність технічних дій.

MTTD обчислюється лише для виявлених інцидентів, тому його необхідно інтерпретувати разом із Recall і FN. Низьке значення MTTD не є ознакою належної роботи, якщо значна частина інцидентів не була виявлена. MTTR також не характеризує невиявлені інциденти, для яких реагування не розпочиналося.

Ретроспективні дані, наведені у попередньому підрозділі, відповідають визначеним напрямам впливу: у періоди масових відключень електропостачання MTTD збільшувався більш ніж у п'ять разів, MTTR — приблизно на чверть, а доступність технологічної платформи SOC зменшувалася [49]. Ці значення підтверджують напрям залежностей, але не використовуються як універсальні коефіцієнти.

2.1.5. Інтегральне представлення та межі моделі

Результуючий стан процесів обробки подій безпеки на визначеному часовому інтервалі подається вектором основних показників:

$$Y = [Lobs, NI, FP, FN, Accuracy, Recall, MTTD, MTTR] \quad (2.7)$$

Фактори воєнного середовища спочатку змінюють Lobs, аналітичне навантаження Q та доступність реагування R. Ці проміжні стани визначають значення компонентів Y. Таким чином, модель відображає не прямий зв'язок між відключенням електроживлення та окремою метрикою, а послідовний механізм: відключення спричиняє втрату джерел і контексту; Lobs зростає; збільшуються FP, FN, MTTD і MTTR; Recall та Accuracy зменшуються. Інтенсифікація атак додатково збільшує фактичну кількість інцидентів і навантаження.

Параметри моделі визначаються окремо для конкретної інфраструктури. Базові значення обчислюються за періодами відносно стабільної роботи. Коефіцієнти впливу можуть бути встановлені експертно, за ретроспективними спостереженнями або за результатами контрольованого експерименту [59]. Для практичного застосування достатньо порівнювати базовий і деградований стани за однаковими правилами обчислення метрик.

Запропонована модель є загрубленою. Вона не прогнозує дії загрозового агента, не визначає точну кількість майбутніх інцидентів і не враховує всі організаційні взаємозалежності SOC. Її призначення полягає у формальному поданні основного механізму впливу: деградація інфраструктури збільшує втрату спостережності, яка погіршує якість класифікації та часові характеристики виявлення і реагування.

Для обчислення Lobs необхідне актуальне представлення джерел телеметрії, активів, їх географічної приналежності, каналів зв'язку, резервування та взаємозалежностей. Статичний реєстр не забезпечує належної якості таких даних у середовищі інтенсивних змін. Тому подальша розробка методів повинна спиратися на формалізований процес управління активами безпеки (Security Asset Management, SAM), багатоджерельне злиття даних та контроль їх часової актуальності [49].

Метрика Lobs використовується як основний показник стану спостережності, а FP, FN, Accuracy, Recall, MTTD і MTTR — як критерії експериментального порівняння базового та запропонованого підходів. Це забезпечує достатню формальність моделі без надмірного ускладнення математичного апарату.

2.2. Схема управління активами з врахуванням динамічності та резервування інфраструктури

Схема процесу управління безпековими активами орієнтується на повну ідентифікацію активів інформаційної інфраструктури з рівнем деталізації, визначеним технічними вимогами. Ідентифікація трактується як відображення кожного активу у множині впорядкованих атрибутів, достатніх для подальшого застосування політик безпеки, контролів моніторингу та процедур реагування. Семантично актив розглядається як кортеж $a = \langle id, C, \mathcal{A}(t) \rangle$, де id — унікальний ідентифікатор; C — клас (наприклад, сервер, робоча станція, мережевий пристрій, компонент технологій виробництва (Operational Technologies, OT), програмна система чи інформаційно-технологічний сервіс);

$\mathcal{A}(t)$ — часово залежний набір атрибутів. До таких атрибутів належать мережеві реквізити (IP-адреси, повні доменні імена (Fully Qualified Domain Name, FQDN), ідентифікатори віртуальних локальних мереж (VLAN), MAC-адреси), ознаки платформи (тип та версія операційної системи, склад програмного забезпечення, рівень інсталяції оновлень безпеки), стан покриття засобами антивірусного захисту, статус та часові метрики останнього сканування у межах процесу керування вразливостями, а також організаційні атрибути (власник, належність до бізнес-системи чи сервісу).

Інфраструктура моделюється як позначений орієнтований граф вершини якого відповідають активам, а ребра — відношенням функціональної або мережевої залежності. Оскільки у воєнний період спостерігаються інтенсивні зміни топології, підтримання інвентаризації є задачею безперервної оцінки стану. Практично це означає, що джерело істини щодо складу активів не може бути статичним: репрезентативність і довіра до будь-якого реєстру суттєво знижуються в короткостроковій перспективі без автоматизованого оновлення. З огляду на зазначене, процес SAM має реалізовувати багатоджерельне оцінювання злиттям даних (data fusion). Конкретні теоретичні та практичні вимоги щодо реалізації даної функції лежить за межами тематики даного дослідження [60].

В умовах неповної синхронізації, характерної для переривчастої зв'язності середовища, а також проблематику можливої реалізації загроз в середовищі, модель даних інвентаризації має підтримувати події з відкладеною доставкою та монотонні оновлення.

У воєнний час вимоги до автоматизації зростають як через швидкість змін, так і через дефіцит кадрів та необхідність роботи під обмеженнями доступності. Тому принципи SAM повинні забезпечувати: переважання машинних джерел спостереження над ручними реєстрами; пріоритезацію джерел із різною природою спостереження (мережеве спостереження, системи керування, реєстри конфігурацій), щоб мінімізувати перетини відмов; буферизацію телеметрії поза центром мережі з подальшим узгодженням після

відновлення зв'язності; формальну модель довіри до джерел, у якій вага джерела є функцією свіжості, покриття та історичної точності [61].

Ці міркування підводять до вибору класів інвентаризаційних джерел. Необхідний незалежний шар зовнішнього спостереження за фактами існування та стану вузлів у мережі. Він має забезпечувати безперервне виявлення, підтвердження доступності та первинну атрибутику навіть за відмов окремих систем обліку; додатково, завдяки об'єктивній природі збору даних, цей шар знижує ризик систематичних помилок. По-друге, необхідний авторитативний шар нормативної конфігураційної істини для систем і сервісів, який задає цільовий склад активів, їх ролі, залежності та життєвий цикл; саме цей шар забезпечує відповідність між технічною та організаційною моделями. По-третє, потрібен шар ідентичностей і облікових записів як джерело правди про належність, стан увімкнення, політики доступу й фактичну активність об'єктів обліку; він дає можливість корелювати мережеві спостереження з організаційними сутностями та виявляти “сірі” активи (невраховані системи, тіньова ІТ-активність) [62].

У поєднанні вказані вище джерела інвентаризації формують мінімальний достатній базис для багатоджерельного злиття: вони є ортогональними за природою вимірювання, статистично комплементарними для евристичного підсилення довіри до атрибутів, стійкими до спільних відмов у середовищі з переривчастою зв'язністю та вимушеним резервуванням [60]. Конкретними реалізаціями джерел є:

- Мережевий сканер з доступом до усіх мережевих сегментів в розподіленій чи централізованій архітектурі. Задачею мережевого сканера є виявлення на постійній основі мережевих активів та їхні сервіси, а також ідентифікація порушень мережевої зв'язності між великими сегментами мережі. Застосування сканера дозволяє досягти виявлення фактичних змін в інфраструктурі та порушень доступності ІТ-систем.
- Configuration Management Database (CMDB) з інформацією по структурі відповідальності за окремі сегменти та ІТ-сервіси. Дана теза може

здаватись протиречною з урахуванням того факту, що системи класу CMDB зазвичай наповнюються вручну, однак такою не є. Не зважаючи на швидкі зміни в інфраструктурі, зазвичай відносно великі сегменти мережі та IT-сервіси не змінюються швидко, як і відповідна структура відповідальності. Витрати часу та ресурсів на підтримку даних про відповідальність та розподіл IT-сервісів по великим фрагментам інфраструктури є відносно невеликими у порівнянні з актуалізацією таких даних щодо кожного окремого атомарного активу.

- Система централізованої аутентифікації або служба каталогів – такі, як Microsoft Active Directory. Рішення має охоплювати більшість інфраструктури та підтримувати облік, автоматичну актуалізацію інформації та керування більшою частиною інфраструктури. З огляду на різноманітність типів пристроїв та систем, що можуть існувати в інфраструктурі, очевидно, що система не буде покривати усі активи, однак буде надавати найбільший обсяг даних в порівнянні з іншими об'єктивними джерелами даних, не потребує додаткового впровадження виключно з потреб безпеки та здебільшого не залежить від перебоїв доступу до хмарних технологій.

Здебільшого джерелами інформації про хмарні частини інфраструктури можуть виступати ті ж засоби, що були наведені для наземної, однак, очевидно, що специфіка хмарних технологій передбачає складнощі в ідентифікації компонентів Platform-as-a-Service (PaaS) та Software-as-a-Service (SaaS) практично будь-якими наведеними вище засобами. Також складність передбачає можливість розриву інтернет-зв'язку між майданчиками інфраструктури наземної хмарної внаслідок реалізації військових ризиків. В свою чергу, ефективним засобом ідентифікації хмарних активів виступають технології класу Cloud-Native Application Protection Platform (CNAPP). Ключовою вимогою до такої технології є інтеграція з панелями керування провайдерів публічних хмарних послуг (Amazon AWS, Microsoft Azure, Google GCP, тощо), збір інформації про підключені сервіси та об'єкти, а також їхню конфігурацію. За умови розгортання відповідного технологічного рішення усі

нові хмарні об'єкти, що будуть підключені до інфраструктури будуть автоматично ідентифікуватись та долучатись до інвентаризації в рамках SAM при підключенні рішення до відповідної системи інвентаризації [63] [58].

У попередньому розділі встановлено, що низка метрик SOC-CMM є чутливими до специфічних викликів військового часу. Це вимагає акумуляції таких інвентаризаційних змінних стану активів, які прямо завбезпечують визначення операційної ефективності: з них будуть будуватись контролі та індикатори ефективності процесів безпеки. Атрибути мають: зменшувати невизначеність щодо наявності та досяжності активу (вплив на “простій джерел подій), пояснювати зміни у виявленні та реагуванні (вплив на середній час виявлення/реагування), підтримувати ризик-орієнтовану пріоритезацію ресурсів (вплив на черги опрацювання, перевантаження змін, відсоток хибних спрацювань), коригувати планування резервів та відновлення (вплив на доступність технологій і середній час між інцидентами).

У межах моделі процесу до активів (атомарних і комплексних, зокрема інформаційних систем та сервісів) прив'язуються атрибути вказані в таблиці 4 [58]:

Таблиця 4 - специфічні калькульовані атрибути активів [58]

Атрибут	Семантика
Динамізм активу	Індикатор чутливості технічних і мережевих характеристик до втрати електроживлення та зв'язності; підвищений динамізм корелює зі зростанням латентності спостереження, що напряду впливає на середній час виявлення та кількість пропущених інцидентів.
Рівень резервування електроживлення	Мінімальний гарантований інтервал автономної роботи; слугує предиктором доступності телеметрії та зменшує простої джерел журналів, тим самим стримуючи деградацію видимості.

Рівень резервування зв'язку	Мінімальний гарантований інтервал збереження зовнішньої мережевої досяжності за відмови основного каналу; визначає сталість каналів кореляції подій і дистанційних дій реагування.
Кількість резервних каналів зв'язку	Кількість незалежних транспортних маршрутів; визначає ймовірність спільної відмови.
Час останньої ідентифікації та час останньої успішної ідентифікації	Часові мітки для оцінки актуальності даних; розрив між ними є індикатором якості спостереження і застосовується як ваговий коефіцієнт у кореляційних правилах та фільтрах виявлення втрати актуальності атрибутів. Різниця даних показників відображає можливі втрати доступності об'єкту.
Історія змін	Журнал подій щодо змін значущих атрибутів (append-only) для відстеження стрибкоподібних зсувів стану; забезпечує відтворюваність розслідувань і покращує середній час аналізу шляхом автоматичної реконструкції контексту.
Географічна приналежність	Просторовий дескриптор із вказанням гранулярності (точна/орієнтовна) - необхідний для просторових політик реагування, оцінювання ризиків на рівні майданчиків і кореляції з подіями фізичної безпеки, що впливає на середній час локалізації та інтервал між інцидентами.
Дескриптор загроз	Синтетична змінна, сформована з відомостей про роль активу, його експозицію та відображення на техніках методологічній рамці MITRE ATT&CK®; використовується для пріоритезації обробки сповіщень і відпрацювання контрольних дій, зменшуючи частку хибних позитивних результатів і пришвидшуючи реагування.

Обчислення названих атрибутів здійснюється на основі інвентаризаційних даних і стандартизованих процедур ідентифікації для комплексних активів; технічні засоби збору та імплементації не деталізуються у цій роботі. Зазначений набір є мінімально достатнім для побудови контрольних функцій і метрик у подальшому розділі, оскільки забезпечує математично обґрунтований зв'язок між спостережністю, доступністю телеметрії та часовими метриками ефективності SOC-процесів, які особливо варіативні у воєнних умовах [58] [64].

Динамізм активу доцільно розглядати не як властивість кіберзагрози, а як формалізовану характеристику поведінки об'єкта інфраструктури в умовах зміни стану середовища виконання. У межах моделі управління безпековими активами SAM динамізм активу визначається як інтегральний показник нестабільності його стану, ідентифікаційних ознак, мережевої досяжності та топологічних залежностей за умов деградації електроживлення, каналів передавання даних або реконфігурації мережевої структури. Показник характеризує очікувану складність коректного відображення цього активу у поточній моделі інфраструктури [58].

Актив може бути поданий як об'єкт із часово залежним вектором атрибутів. До цього вектора належать ідентифікатори вузла, мережеві адреси, роль у графі залежностей, стан телеметричних каналів, параметри резервування, історія змін конфігурації та часові мітки останнього підтвердження. Динамізм відображає інтенсивність і потенційну невизначеність змін цього вектора. Низький рівень динамізму характерний для об'єктів зі стабільною адресацією, контрольованим життєвим циклом і достатнім резервуванням. Високий рівень динамізму характерний для вузлів із волатильною конфігурацією, залежністю від непостійної мережевої зв'язності, частими змінами ідентифікаторів або відсутністю стійкого джерела підтвердження стану.

У графовій моделі інфраструктури динамізм активу визначає ймовірність зміни властивостей вершини або суміжних ребер протягом обмеженого часового інтервалу. Якщо актив втрачає електроживлення, змінює точку підключення, отримує іншу IP-адресу, втрачає агент телеметрії або тимчасово випадає з області сканування, то його відповідність попередньому інвентаризаційному запису стає неочевидною. Поняття динамізму можливо формалізувати до (1):

$$D(a) = \frac{1}{m} \sum_{i=1}^m d_i(a) \quad (1) [65]$$

де m - кількість атрибутів активу, d - нормований до $[0,1]$ динамізм кожного атрибуту [65].

Дескриптор загроз доцільно визначати як синтетичний атрибут активу, що формує формалізоване подання його потенційної релевантності для реалізації типових сценаріїв дій супротивника. дескриптор загроз агрегує семантичні ознаки активу: функціональну роль у системі, мережеву експозицію, місце у графі залежностей, критичність для бізнес-сервісів, доступність засобів реагування та відповідність відомим тактикам і технікам матриці MITRE ATT&CK, що зумовлює певну відмінність від базових інвентаризаційних атрибутів, які описують технічний стан активу.

У межах моделі SAM дескриптор загроз є похідним вектором ознак, який обчислюється на основі канонічного запису активу та контексту його використання. До вхідних параметрів можуть належати клас активу, роль, сегмент мережі, тип доступу, наявність зовнішньої експозиції, зв'язки з іншими активами, належність до сервісної групи, критичність, історія спостережуваних подій, покриття засобами захисту та доступні механізми локалізації. Результатом є не одиничне текстове поле, а структуроване представлення, придатне для алгоритмічної обробки в системах кореляції, пріоритезації та планування контролів. Дескриптор загроз можна інтерпретувати як функцію відображення активу з простору інфраструктурних ознак у простір загрозових сценаріїв. Якщо актив подано як вершину позначеного орієнтованого графа

інфраструктури, то дескриптор загроз характеризує множину можливих ролей цієї вершини в траєкторіях атаки: початкова точка доступу, проміжний вузол латерального переміщення, джерело привілейованих облікових даних, ціль ексфільтрації даних, елемент керування або компонент, порушення якого впливає на доступність сервісу [65].

Відображення на MITRE ATT&CK у цьому випадку виконує роль таксономії поведінкових шаблонів супротивника. Для кожного активу визначається множина релевантних тактик і технік, які є правдоподібними з огляду на його роль, експозицію та доступні інтерфейси. Наприклад, для контролера домену релевантними будуть техніки, пов'язані з доступом до облікових даних, підвищенням привілеїв і латеральним переміщенням; для публічного веб-сервера - техніки початкового доступу, виконання коду та закріплення; для мережевого пристрою - техніки маніпуляції трафіком, порушення доступності та ухилення від виявлення [65].

Дескриптор загроз зменшує невизначеність під час обробки подій, оскільки додає до телеметрії знання про те, які типи подій є очікувано значущими для конкретного активу. Однакова подія на різних активах може мати різну операційну вагу. Наприклад, спроба віддаленого входу на робочу станцію користувача, сервер прикладного рівня та вузол адміністрування не повинна мати однакою пріоритетність, оскільки ці активи відрізняються роллю у графі доступів і потенційними наслідками компрометації. Дескриптор загроз дає змогу формалізувати цю різницю без ручного аналізу кожного окремого випадку. Дескриптор загроз може бути формалізований як (2):

$$\Theta(a) = (R(a), E(a), K(a), T(a)) \quad (2) [65]$$

, де R - роль активу, E - експозиція (ступінь доступності для порушника), K - критичність, T - бінарний вектор релевантності технік з моделі Mitre Att&ck. Асоціація динамізму активу з пов'язаним ризиком будується на основі твердження про зворотню залежність спостережності активів під час глобальних перебоїв електроживлення та зв'язку від рівня динамізму активу, що відповідно впливає на процеси виявлення та реагування на інциденти [65].

2.3. Дескриптивна модель формування методів покращення спостережності

Було застосовано методологію розроблення методів для SOC, спрямованих на мінімізацію наслідків зниження рівня видимості та спостережності під час відключень електропостачання. Методологія структурована навколо чотирьох базових дій (рис. 2) [67].

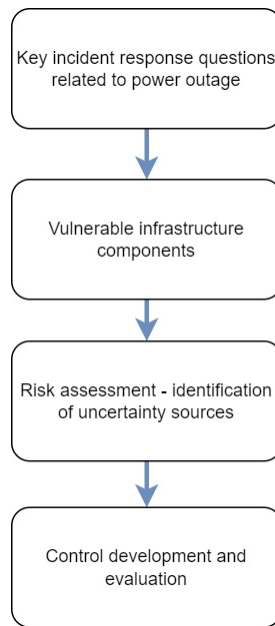


Рисунок 2. Методологія формування методологічної рамки прикладних сценаріїв [67]

Відмінність процесу реагування в зазначених умовах полягає у зростанні невизначеності щодо першопричини зафіксованих аномалій. Команди реагування на комп'ютерні інциденти безпеки повинні мати змогу надати відповідь на наступні питання щодо інциденту [67]:

- Чи є втрата зв'язності з окремими пристроями виключно наслідком відключення електропостачання, чи вона зумовлена навмисним втручанням злоумисника?
- Чи обумовлені розриви в журналах подій перебуванням систем у вимкненому стані, чи журнали були навмисно змінені або видалені з метою приховування слідів атаки?

- Чи відображають аномальні мережеві поведінкові характеристики автоматичні процеси повторного підключення після відновлення живлення, чи вони є індикаторами поширення шкідливого програмного забезпечення або латерального переміщення суб'єкта загрози [67]?

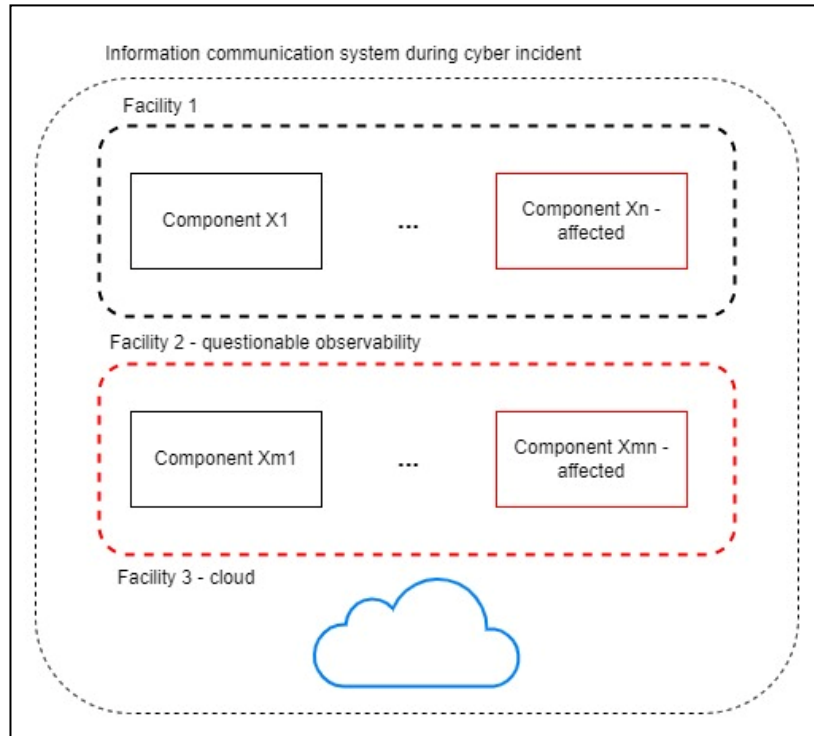


Рисунок 3 - Узагальнена схема типової інфраструктури за умов втрати спостережності [67]

Нездатність коректно диференціювати зазначені сценарії, як відображено на рис.3, може призвести або до пропуску реальних інцидентів інформаційної безпеки та несвоєчасного реагування, або до нераціонального розподілу ресурсів унаслідок обробки хибнопозитивних подій, спричинених відключенням електропостачання [67][68].

2.3.1. Ідентифікація вразливих компонентів інфраструктури

На цьому етапі було сформульовано та ідентифіковано компоненти інфраструктури, які є найбільш уразливими з точки зору втрати видимості та спостережності під час відключень електропостачання. Ідентифікація здійснювалася шляхом виконання системного аналізу відповідно до переліку операцій, наведених у таблиці 5.

Таблиця 5 - операції в рамках ідентифікації вразливих до втрати спостережності компонентів інфраструктури [67]

Операція системного аналізу	Опис
Оцінювання інфраструктури	Проведення комплексного аналізу наявних інфраструктур досліджуваних організацій — енергетичної компанії, фінансової установи та державного органу, розташованих на території України та таких, що функціонують в умовах регулярних відключень електропостачання, спричинених руйнуванням енергетичної інфраструктури.
Ідентифікація критичних систем	Визначення ключових систем та активів, що мають суттєве значення для моніторингу безпеки та реагування на інциденти, зокрема: засобів мережевого моніторингу, сенсорів безпеки, механізмів журналювання подій, систем комунікації та центрів обробки даних.
Аналіз вразливостей	Оцінювання впливу відключень електропостачання на визначені компоненти з урахуванням їх залежності від безперервного електроживлення, рівня резервування, а також географічної розподіленості, що ускладнює технічне обслуговування та оперативне реагування.

2.3.2. Оцінювання ризиків та формування джерел невизначеності спостережності під час реагування

На основі проведеного дослідження компонентів інфраструктури та аналізу їх специфічних вразливостей до втрати спостережності було ідентифіковано та формалізовано базові узагальнені ризики, які впливають на рівень видимості та спостережності. Розуміння характеру впливу порушень електроживлення на кожний об'єкт інфраструктури дозволило локалізувати потенційні зони втрати спостережності та визначити можливості їх компенсації за рахунок змін підходів до моніторингу [67].

За результатами узагальненого оцінювання ризиків визначено специфічні слабкі місця інфраструктури, які можуть слугувати диференційними індикаторами між активністю зловмисника та аномаліями, зумовленими відключенням електропостачання. На основі даних результатів розроблено набір моніторингових контролів, орієнтований на цілеспрямоване виявлення та мінімізацію зазначених ризиків. Запропоновані контролі адаптовані для детекції розбіжностей між типовими операційними аномаліями, спричиненими перебоями електроживлення, та шкідливою активністю агента загрози [67].

Після впровадження ефективність запропонованого набору прикладних сценаріїв оцінюється кількісно. Ключовим цільовим показником є середній час реагування (Mean Time to React, MTTR) для інцидентів, що загально опрацьовуються в SOC. Показник MTTR є ключовим індикатором ефективності процесів реагування. Його зменшення свідчить про підвищення здатності системи до своєчасної ідентифікації та оброблення інцидентів із мінімізацією потенційних наслідків. Однак в рамках експериментального дослідження в синтетичних умовах відтворити динаміку операційного показника MTTR з достатньою мірою достовірності не представляється можливим, внаслідок відсутності суб'єктів реагування як таких. Натомість, в якості проміжної метрики, яка впливає на час реагування, виявлення та інші ключові показники на пряму [67], та, в той же час, є достовірно вимірюваною в межах експерименту, береться показник загальної кількості виявлених порушень, показник кількості

хибнопозитивних порушень та їх відсоткове співвідношення (False Positive Rate) [67].

2.3.3. Результати ідентифікації ризиків

На основі високорівневого оцінювання ризиків було визначено ключові ризики, які можуть бути мінімізовані шляхом впровадження спеціалізованих моніторингових сценаріїв у процесі реагування на кіберінциденти. Зазначені ризики зумовлені тим, що відключення електропостачання маскують реальну природу системних і мережевих аномалій, ускладнюючи розмежування між подіями, спричиненими втратою живлення, та подіями, зумовленими шкідливою діяльністю (рис. 4), і формалізовані в таблиці 6 [67].

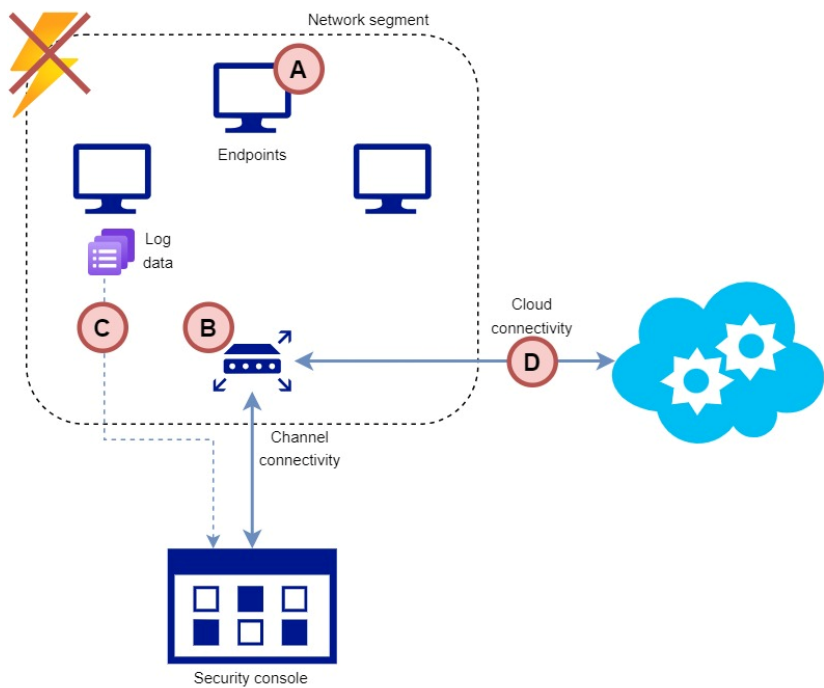


Рисунок 4 - Узагальнена схема змодельованої інфраструктури з відображенням оцінки пов’язаних ризиків, де А, В, С, D — ідентифіковані ризики [67]

Таблиця 6 - Ідентифіковані ризики втрати спостережності для змодельованої інфраструктури та їх вплив на видимість системи [67]

Ризик	Опис	Вплив
-------	------	-------

Ризик помилкової інтерпретації знеструмлених вузлів як скомпрометованих систем	Під час відключення електропостачання комп'ютери та сервери можуть бути недоступними виключно через відсутність живлення. Недоступність може бути хибно інтерпретована як наслідок компрометації, зокрема шифрування, навмисного вимкнення або іншого зловмисного впливу.	Неправильне встановлення причини недоступності призводить до неефективного реагування. Ресурси можуть бути спрямовані на розслідування неіснуючого інциденту, тоді як реальна атака може залишитися непоміченою у випадку її помилкового віднесення до наслідків відключення електропостачання.
Ризик помилкової інтерпретації знеструмлених мережевих сегментів як результату мережевої атаки	Мережеві сегменти можуть втратити доступність через відключення живлення комутаторів, маршрутизаторів або інших компонентів мережевої інфраструктури. Втрата зв'язності може бути сприйнята як наслідок мережевої атаки, наприклад порушення конфігурації, примусового вимкнення каналів зв'язку, атаки типу Distributed Reflection Denial of Service (DRDoS) або	Неправильна діагностика мережевої недоступності може призвести до затримки або неадекватності заходів реагування. Команда безпеки може ініціювати надмірні контрзаходи, не виявити реальну атаку або несвоєчасно відновити мережеві сервіси.

	маршрутизаційних і спуфінгових атак.	
Ризик помилкової інтерпретації втрати журналів через знеструмлення як їх навмисного видалення	Раптове вимкнення систем унаслідок відключення електропостачання може спричинити неповне збереження або пошкодження файлів журналів подій. Така втрата може бути сприйнята як навмисне видалення або модифікація журналів з метою приховування слідів атаки.	Невірна інтерпретація причин втрати журналів ускладнює форензичний аналіз і затримує ідентифікацію інциденту. Одночасно існує ризик пропуску реальної компрометації у випадку автоматичного віднесення втрати журналів до наслідків відключення живлення.
Ризик недостатньої обізнаності щодо наявних можливостей реагування	Відключення електропостачання можуть впливати на функціональний стан засобів кіберзахисту. Невизначеність щодо фактичної працездатності цих засобів знижує керованість процесу реагування..	Відсутність чіткої інформації про доступність засобів захисту призводить до невикористання наявних механізмів стримування та ліквідації загроз та формування прогалин в захисті, продовжує тривалість реагування на інциденти і збільшує потенційний масштаб збитків.

2.4. Методи обробки подій безпеки призначені для покращення спостережності інформації в ІКС

Для кожного ідентифікованого ризику запропоновано метод, спрямований на часткову мінімізацію відповідного ризику та підвищення рівня видимості інфраструктури.

2.4.1. Контроль змін стану живлення та відновлення стану системи (Power status changes control)

Моніторинговий сценарій, орієнтований на аналіз поведінки завершення та відновлення роботи кінцевих вузлів. Контроль визначає, чи відбулося коректне (graceful) завершення роботи, чи вузол було вимкнено аварійно.

Логіка контролю базується на припущенні, що під час раптового відключення електроживлення система зазвичай не формує подій коректного завершення роботи, а відсутність ознак аварійного відновлення після запуску свідчить про коректне завершення роботи. Натомість наявність відповідних записів у журналах подій свідчить про ініціювання штатної процедури завершення (користувачем або автоматизованим сценарієм), за винятком випадків застосування джерел безперебійного живлення (Uninterruptible Power Supply, UPS), що дозволяють виконати контрольоване завершення. Наявність процедур відновлення або системних помилок при запуску вказує на раптове вимкнення, зумовлене втратою живлення або апаратною відмовою. Кореляція подій завершення роботи дозволяє розмежувати аварійні вимкнення та навмисні або штатні дії оператора [67].

2.4.2. Контроль доступності каналів зв'язку (Communication channel availability control)

Сценарій, спрямований на перевірку функціонування мережевих каналів, що з'єднують віддалені географічно розподілені сегменти інфраструктури. Перевірка здійснюється шляхом ICMP-запитів, TCP-проб або інших методів тестування доступності VPN-з'єднань, SD-WAN-мереж або каналів до хмарних провайдерів.

Втрата зв'язності ініціює сповіщення для подальшого аналізу причин, включаючи можливі несанкціоновані зміни конфігурації мережевого обладнання або цілеспрямовані кібератаки. Контроль доповнює механізми моніторингу доступності кінцевих вузлів [67].

2.4.3. Контроль аномалій оренди DHCP (DHCP leasing anomaly control)

Моніторинговий сценарій, орієнтований на виявлення аномалій у процесах видачі IP-адрес за протоколом Dynamic Host Configuration Protocol (DHCP). Контроль аналізує інтенсивність та частоту запитів і видач оренд, виявляючи різкі сплески або зниження активності.

Різке збільшення кількості запитів може свідчити про масове перезапускання пристроїв після відновлення живлення. Контроль дозволяє відрізнити такі сценарії від підключення несанкціонованих пристроїв або зловмисної активності, а також забезпечує цілісність історії призначення IP-адрес для цілей цифрової криміналістики [67].

2.4.4. Контроль змін конфігурації обладнання (Hardware configuration changes control)

Сценарій моніторингу змін конфігурації мережевого та, за можливості, енергетичного обладнання. Контроль відстежує зміни параметрів маршрутизаторів, комутаторів, міжмережевих екранів, а також UPS.

У разі виявлення аномалії доступності контроль перевіряє наявність нещодавніх змін конфігурації, що могли спричинити інцидент, що забезпечує диференціацію зловмисних дій від легітимних адміністративних змін [67].

2.4.5. Контроль стану живлення мережевого сегмента (Network segment power status control)

Сценарій, що базується на використанні контрольного пристрою, підключеного до автономного джерела живлення. Порівняння його доступності з доступністю інших пристроїв сегмента дозволяє встановити факт відключення електропостачання на локації.

Одночасна недоступність більшості пристроїв при збереженні доступності контрольного вузла інтерпретується як відключення живлення, а не як кібератака або мережевий збій [67].

2.4.6. Контроль цілісності та повноти журналів (Log data integrity control)

Сценарій, спрямований на виявлення спроб модифікації, видалення або інших порушень безперервності журналювання подій. Контроль передбачає аналіз системних подій очищення журналів та застосовує часову кореляцію щодо перерв у надходженні подій. Якщо тривалість перерви перевищує очікуваний період відсутності живлення або виникає без відповідного підтвердження аварії, ініціюється розслідування щодо можливого втручання в механізми журналювання [67].

Наявність неочікуваних розривів у надходженні телеметрії або змін часових міток дозволяє відрізнити втрату даних через відключення живлення від навмисного приховування слідів компрометації [67].

2.4.7. Контроль доступності хмарних агентів (Cloud agents uptime control)

Моніторинговий сценарій перевірки активності агентів захисних рішень, що взаємодіють із централізованими хмарними платформами. Даний контроль забезпечує розуміння фактичної доступності засобів реагування в умовах інциденту. SOC має змогу оцінити поточні технічні можливості стримування та ліквідації загроз з урахуванням впливу відключення електропостачання або інших порушень функціонування інфраструктури [67].

2.4.8. Метод ідентифікації втрати спостережності

Використання пари атрибутів розширеної інвентаризації «Час останньої ідентифікації та час останньої успішної ідентифікації» дозволяє виявити факт втрати спостережності активу. Якщо остання спроба ідентифікації пройшла пізніше ніж остання успішна ідентифікація за одразу всіма джерелами, можна вважати, що спостережність активу втрачено. Кореляція даної події з подіями,

що можуть свідчити про зникнення електроживлення з інших джерел (наприклад, з джерела безперебійного живлення) , дозволяє чітко ідентифікувати факт та обсяг відключення. Використання даної інформації в якості події ІБ в інших контролях та кореляційних правилах може суттєво зменшити кількість хибнопозитивних спрацювань. В свою чергу, кореляція даної події з фактом приналежності активу до небезпечного географічного регіону (атрибут «Географічна приналежність») дозволяє виявити втрату спостережності внаслідок бойових дій [67].

2.4.9. Фільтр динамізму активу

Атрибут динамізму активу визначає «вразливість» спостережності активу до втрати, перш за все, електроживлення. Якщо актив є динамічним – відповідно відслідковування змін його динамічних атрибутів не матиме сенсу при наявності факту підтвердженого відключення електропостачання у визначений період часу. Таким чином кореляційна логіка контролів, спрямованих на відслідковування змін чи відсутності змін динамічних атрибутів може бути доповнена фільтром динамізму. Яскравим прикладом може бути контроль зміни волатильної конфігурації мережевих пристроїв (там, де конфігурація є енергозалежною). Після зникнення електроживлення активу, усі такі конфігурації будуть автоматично знищені, відповідно після його відновлення відповідні контролі будуть генерувати сповіщення щодо неавторизованої зміни конфігурації. При цьому не всі мережеві пристрої мають енергозалежну конфігурацію – відповідно, додавання у контроль логіки виключення усіх пристроїв при відключенні електропостачання не буде коректним. Застосування такого механізму дозволяє зменшити відсоток хибнопозитивних спрацювань (Percentage of False Positive alerts), та непрямо позитивно впливатиме на показники, пов'язані з часовими метриками опрацювання інцидентів, а також на показник Overbooked time [58].

2.4.10. Контроль динамічного впливу

Контроль передбачає виявлення факту суттєвого впливу на спостережність тієї чи іншої групи активів. Логіка контролю полягає в

виявленні події відключення електропостачання для групи об'єктів (комплексного активу, ІТ-сервісу, ІТ-системи), та кореляції даної події з наявністю відносно великого відсотка динамічних активів в групі. Відсоток динамічних об'єктів, який має викликати спрацювання визначається індивідуально, може залежати від конкретних вимог ІБ щодо спостережності, ризик-апетиту, тощо. Спрацювання контролю та відповідна подія дозволяють підрозділу ІБ ідентифікувати факт суттєвого впливу на спостережність інформації в сегменті на певний період, що при реагуванні на інцидент може бути враховано для збереження часу та, в свою чергу, застосування методів ручного пошуку підозрілих активностей в проблемних сегментах. Застосування контролю впливає на зменшення False-Negative Rate, дозволяючи уникнути фактичних прогалин в детектуванні інцидентів [58].

2.4.11. Метод застосування метрики відповідності захисту об'єкту профілю загроз

Метрика оцінює ступінь покриття об'єкта засобами спостережності відносно релевантних для нього тактик і технік MITRE ATT&CK з урахуванням їхнього ризикового пріоритету. Для об'єкта формується зважений перелік технік, кожна техніка вважається покритою, якщо існує щонайменше одне надійне джерело спостережності або правило виявлення, а за умов перебоїв покриття масштабується часткою фактичної доступності джерела за період. Значення метрики представляє собою зважену частка покритих технік у відсотках, де 100% означає повну практичну спостережність. додатково визначається «розрив покриття» та ранжуються найбільші прогалини за внеском у ризик для активу. Алгоритм розрахунку зводиться до профілювання загроз, відображення джерел на техніки, урахування доступності. Ключовою метою застосування метрики є підвищення видимості MITRE ATT&CK, зменшення частки пропущених інцидентів і скорочення середнього часу виявлення інцидентів; для контролю доцільно відстежувати метрику як плаваюче середнє з порогами для критичних об'єктів [58].

2.4.12. Метод пріоритизації операцій Threat Hunting як ручної перевірки наявності потенційних загроз.

Використання метрики відповідності захисту профілю загроз дозволяє оцінити рівень спостережності об'єкта щодо пріоритетних тактик і технік (ТТР) та обґрунтовано застосовувати Threat Hunting (ТН) як «міжконтрольний» механізм для об'єктів із низьким покриттям і високою цінністю. Оскільки ТН є значно більш трудомісткою процедурою, ніж автоматичні детектуючі контролю, доцільною є її пріоритизація виключно для найбільш релевантних систем, де стандартні засоби спостережності є частково недоступними або недостатніми..

Пріоритет і інтенсивність ТН для об'єкта i визначаються індексом [66] де V_i — нормована критичність об'єкта, а C_i — частка покриття релевантних технік АТТ&СК; розподіл часу аналітиків оптимізується в межах доступного ресурсу. Реалізація контролю передбачає встановлення періодичності ТН пропорційно P_i та використання напівнезалежних від платформи SOC методів збору даних (локальна форензика, мережеві дампи, периферійні журнали, ручні кореляції за сценаріями ТТР). Ефективність підходу зростає за умови системного перенесення результатів ТН у вдосконалення журналювання та автоматичних детекцій, що підвищує C_i і зменшує потребу в регулярних ручних сесіях за умов обмежених кадрових ресурсів [58].

2.4.13. Контроль достатнього рівня резервування критичних динамічних систем

На основі атрибутів динамізму, дескриптора загроз активу, атрибутів рівня резервування електроживлення та каналів зв'язку, а також атрибуту рівня критичності активу пропонується контроль достатності резервування критичних сервісів для конкретного активу. Логіка контролю передбачає визначення взаємозв'язку між цінністю активу (рівнем критичності) та рівнем його резервування (комбінація рівня резервування електроживлення та зв'язку), при цьому рівень динамізму активу є мультиплікатором рівня критичності. Чим більшим є рівень динамізму – тим більшим має бути рівень резервування. В рівнянні також враховується коефіцієнт ризик-апетиту. В залежності від його

значення визначається, чи є наявний рівень резервування для активу достатнім, чи ні. Даний контроль реалізує ризик-орієнтований підхід та може застосовуватись для прийняття рішень щодо розгортання додаткових спроможностей резервування. При цьому, контроль передбачає план дій з реагування щодо виявлених невідповідностей, а також план дій щодо критичних активів з високим рівнем динамізму, по відношенню яких було виявлено інцидент, що включав зникнення електропостачання чи зв'язку, та, відповідно, реалізацію динамічності активу. Впровадження даного контролю та всіх додаткових, пов'язаних заходів дозволяє зменшити значення Mean Time Between Incidents та Number of Incidents за рахунок загального зменшення кількості інцидентів – в першу чергу, інфраструктурних [58].

2.4.14. Візуалізація та огляд розроблених методів покращення спостережності

Розроблені методи та контролі, спрямовані на покращення спостережності ІКС в умовах масових відключень електропостачання та інших специфічних військових викликів розв'язують ряд проблем, ідентифікованих в розділі 1. Кожен з запропонованих контролів сфокусований на вирішення частини однієї з чотирьох ключових проблем, при цьому забезпечуючи повноцінне покриття на рівні моніторингу та підтримки спостережності. Зона застосування кожного з контролів відображається на рис. 5.

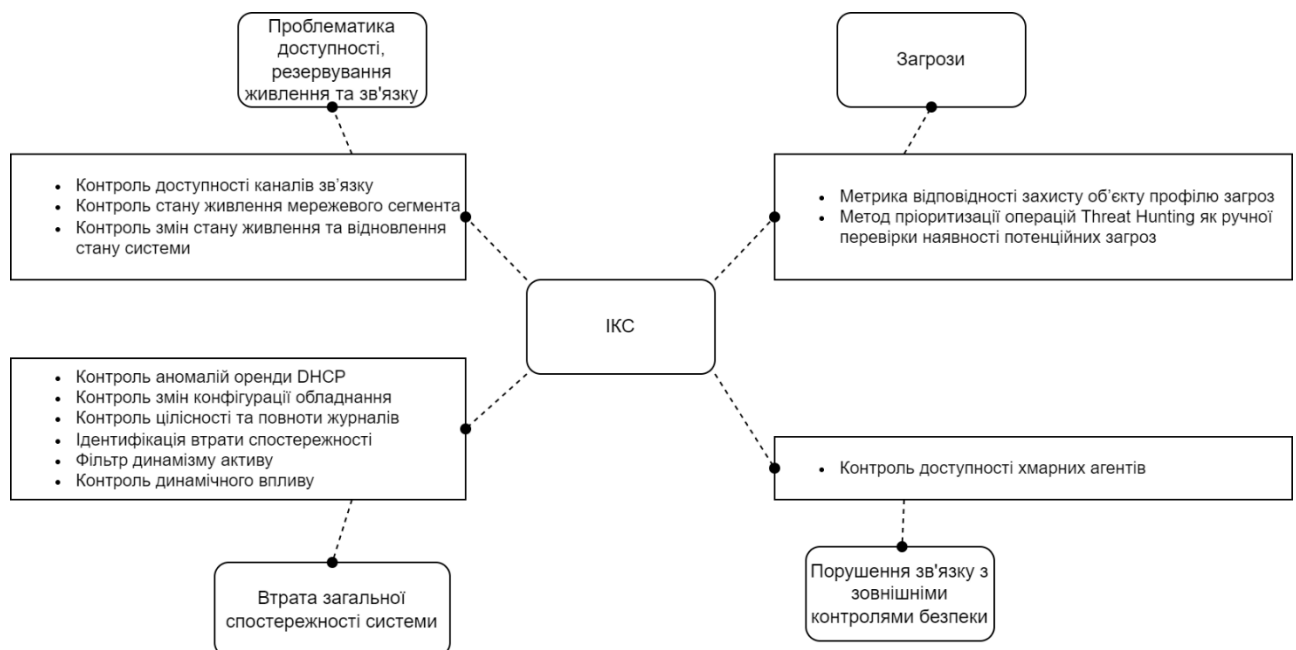


Рисунок 5 - схема застосування запропонованих контролів безпеки для протидії ідентифікованим проблемам спостережності.

Очевидно, що ідентифіковані проблеми спостережності інформації, аналізу даних та прийняття рішень в умовах відключень електропостачання та інших проблем кібербезпеки у військових умовах покриваються запропонованими контролями. Технічна імплементація контролів в процес збору, обробки та аналізу інформації в SOC може дозволити вирішити ідентифіковані проблеми.

Висновки до розділу

У розділі розроблено формалізовану модель впливу деградації інфраструктури на стан спостережності інформації та якість операційної діяльності в комп'ютерних системах управління подіями безпеки. Завдання вирішено шляхом побудови причинно-наслідного відображення «ризиковий фактор - порушений домен керованості - операційна метрика», у межах якого деградація електроживлення, каналів зв'язку, доступності джерел телеметрії, цілісності інвентаризаційних даних і домену довіри проєктується на процеси виявлення, аналізу, реагування, підтримки технологічної платформи та ресурсного забезпечення системи обробки подій безпеки. Як інструментальну основу моделі використано процес управління безпековими активами, у якому актив подається як сукупність атрибутів, важливих з точки зору обліку та мінімізації невизначеності. Результатом виконання завдання є формалізація зв'язку між інфраструктурною деградацією та погіршенням спостережності внаслідок дії факторів військового стану та погіршенням якості операційної діяльності операційних центрів кібербезпеки. Втрата спостережності розглядається як стан системи, що змінює достовірність подій, коректність кореляції, пріоритет розслідувань і допустимі дії реагування. На основі розробленої моделі формалізовано показники за якими вимірюється вплив втрати спостережності на процеси SOC.

У розділі розроблено методи протидії негативним впливам на спостережність інформації військового часу в комп'ютерних системах

управління подіями безпеки. Завдання вирішено через визначення ризиків існуючих методів обробки та аналізу подій безпеки, пов'язаних із втратою спостережності та розробки відповідних методів усунення даних ризиків. Розроблені методи включають в себе алгоритми обробки подій, підходи до кореляції та збагачення подій безпеки. Введено поняття динамізму та дескриптора загроз активу, як атрибутів, що визначають вразливість спостережності активу до інфраструктурної деградації та характерні можливі техніки агентів загроз для реалізації проти активу відповідно. Теоретична основа методів полягає у поєднанні інвентаризаційного контексту активів, оцінки динамізму та дескриптора загроз, та інших важливих з точки зору спостережності ознак деградації телеметрії. Результатом є можливість методологічного переходу від атомарної обробки окремих сигналів до контекстно-залежної інтерпретації подій за якої система розрізняє технічну деградацію, неповноту даних і потенційну активність агента загроз, зменшуючи ризик хибної класифікації стану активів в умовах обмеженої спостережності та під дією воєнних впливів.

РОЗДІЛ 3. РОЗРОБКА АРХІТЕКТУРИ ТА ПРОТОТИПУ ТЕХНІЧНОЇ ІМПЛЕМЕНТАЦІЇ СИСТЕМИ СПОСТЕРЕЖНОСТІ ІКС ТА ЗМЕНШЕННЯ НЕВИЗНАЧЕНОСТІ У ВИЯВЛЕННІ КІБЕРІНЦИДЕНТІВ

3.1. Постановка вимог для розробки системи

3.1.1. Призначення та межі рішення

1.1. Технічне рішення повинно забезпечувати обчислення та використання інвентаризаційних атрибутів активів для побудови моніторингових контролів, орієнтованих на диференціацію аномалій, спричинених деградацією електроживлення/зв'язку, та активності агента загрози.

1.2. Рішення повинно підтримувати безперервне підтримання актуальності інвентаризації активів у середовищі інтенсивних топологічних змін за рахунок багатоджерельного злиття даних (data fusion).

3.1.2. Розподіл функцій між готовими продуктами та власною розробкою

2.1. Компоненти, що доцільно реалізовувати готовими рішеннями:

- SIEM (Security Information and Event Management) як платформа кореляції подій, зберігання подій, детекційних правил, інформаційних панелей і керування кейсами.
- EDR (Endpoint Detection and Response), NGFW (Next-Generation Firewall), UPS/NMS (Uninterruptible Power Supply / Network Management System) як джерела телеметрії та керованих дій реагування (зовнішні системи для здійснення активного реагування).
- CNAPP (Cloud-Native Application Protection Platform) як джерело інвентаризації та конфігурацій публічної хмари (за наявності), з інтеграцією до SAM (опціонально).

2.2. Компоненти, що повинні бути реалізовані на рівні власної розробки (як мінімум у вигляді сервісів/модулів поверх наявних систем):

- ядро SAM (модель активів, залежності, атрибути, історія змін);
- модуль обчислення похідних атрибутів (дескриптор загроз, рівень динамізму);
- модуль збагачення SIEM (enrichment) інвентаризаційними даними;
- Конфігурація SIEM для налаштування відповідних контролів.

3.1.3. Технічний проєкт

Рішення повинно бути реалізоване як сукупність підсистем:

- Підсистема збору та аналізу подій, інцидентів безпеки (SIEM)
- Підсистема активного реагування (EDR): реалізує вимоги алгоритму декомпозиції, оцінювання ізольованості компонентів, технічних механізмів стримування та корекції пріоритезації реагування.
- Підсистема інвентаризації та злиття (SAM Core + Fusion): приймає дані з мережевого сканера, CMDB (Configuration Management Database), служби каталогів (наприклад, Microsoft Active Directory), CNAPP; формує єдине представлення активів і залежностей.
- Модуль обрахунку динамізму: програмний модуль, що використовує дані отримані з підсистеми інвентаризації та злиття для обрахунку атрибуту динамізму активу. Результуючі дані записуються в якості атрибутів SAM та використовуються в інших контролях.
- Модуль обрахунку дескриптора загроз: програмний модуль, що використовує дані отримані з підсистеми інвентаризації та злиття для обрахунку атрибуту дескриптора загроз. Результуючі дані записуються в якості атрибутів SAM та використовуються в інших контролях.
- Підсистема візуалізації та звітності: реалізує візуалізацію ефективності роботи рішення, відображення показників, аномалій, тощо.

Архітектура повинна підтримувати режим неповної синхронізації: відкладену доставку подій та монотонні оновлення інвентаризаційних даних; буферизацію телеметрії поза центром мережі з подальшим узгодженням.

3.1.4. Вимоги до даних та моделей

Модель активу в SAM повинна включати:

- базові мережеві/платформні атрибути (IP, Fully Qualified Domain Name (FQDN), Virtual Local Area Network (VLAN), MAC, операційна система, ПЗ, патч-рівень, покриття засобами захисту тощо);
- часові атрибути ідентифікації (остання спроба/остання успішна ідентифікація) з використанням як коефіцієнтів “свіжості” у правилах кореляції;
- історію змін у форматі append-only;
- атрибути резервування електроживлення/зв’язку та кількість резервних каналів;
- географічну приналежність з ознакою гранулярності;
- “дескриптор загроз” як синтетичну змінну, прив’язану до відображення на техніках MITRE ATT&CK.
- рівень динамізму активу.

Інфраструктура повинна бути подана у вигляді позначеного орієнтованого графа залежностей активів (вершини — активи, ребра — функціональні/мережеві залежності), достатнього для задач декомпозиції та ізоляції компонентів під час реагування.

3.1.5. Вимоги до функцій (контролів) та інтеграції з SIEM

Рішення повинно реалізувати контроль достатності резервування критичних динамічних систем як функцію атрибутів: (критичність, динамізм як мультиплікатор, резервування електроживлення, резервування зв’язку, ризик-апетит), з формуванням плану дій щодо невідповідностей.

Рішення повинно реалізувати метрики резервування активу як нормований показник, придатний для порівняння між класами критичності та оперативного моніторингу в SOC, з використанням атрибутів резервування та потреби активу у зв'язку.

Рішення повинно підтримувати кореляцію подій “зникнення електроживлення” з альтернативних джерел (наприклад, UPS) та з географічною приналежністю для уточнення причин втрати спостережності й зниження хибнопозитивних спрацювань у SIEM.

Рішення повинно підтримувати “фільтр динамізму активу” як умову, що модифікує/відсікає кореляційну логіку контролів у періоди підтверджених відключень електроживлення для динамічних активів.

Рішення повинно підтримувати пріоритезацію ТН на основі індексу, що включає нормовану критичність активу та частку покриття релевантних технік MITRE ATT&CK, з можливістю встановлення періодичності ТН пропорційно індексу.

Рішення повинно забезпечити, щоб усі результати контролів/атрибутів були доступні у SIEM:

- як поля збагачення подій (enrichment) для правил кореляції;
- як окремі синтетичні події (“втрата спостережності”, “недостатнє резервування”, “сегментна деградація спостережності”);
- як інформаційні панелі SOC (KPI, ризикові активи, динамічність/резервування, географічні зрізи).

3.1.6. Вимоги до підтримки реагування (алгоритм декомпозиції та ізоляції)

Рішення повинно забезпечувати процедуру оцінювання здійсненності ізоляції для кожного компонента з урахуванням операційних залежностей і впливу на безперервність бізнес-процесів.

Рішення повинно інтегрувати технічні механізми локалізації (стримування) у вигляді керованих дій (через EDR/NGFW/мережеві засоби), спрямованих на мінімізацію міжсегментного поширення шкідливої активності.

Рішення повинно підтримувати безперервний моніторинг та адаптацію пріоритезації розслідувань відповідно до змін спостережності.

3.2. Архітектура системи

3.2.1. Підсистема збору та аналізу подій, інцидентів безпеки (SIEM)

3.2.1.1. Призначення та межі підсистеми SIEM

Підсистема SIEM призначена для централізованого приймання, нормалізації, збагачення, зберігання та аналітичної обробки телеметрії кібербезпеки з метою формування сигналів про інциденти безпеки, підтримки розслідувань, забезпечення відтворюваності аналітики. У межах даного дослідження SIEM є підсистемою агностичною до конкретної технічної реалізації. Внутрішня архітектура може відрізнятися, однак інтерфейсні та функціональні властивості повинні забезпечувати дотримання вимог, наведених у технічному проєкті.

3.2.1.2. Роль SIEM у логічній архітектурі рішення та вимоги до інтеграції

У технічному проєкті рішення SIEM фіксується як окрема підсистема загальної логічної архітектури; що використовує результати роботи інших підсистем - трьома узгодженими способами: як поля збагачення подій для правил кореляції; як окремі синтетичні події класу «втрата спостережності/недостатнє резервування/сегментна деградація спостережності»; як інформаційні панелі SOC.

Інтерфейсна модель SIEM у межах рішення включає два різні типи вхідних потоків: первинна телеметрія від технічних джерел (журнали; мережеві події; події засобів захисту; події керування інфраструктурою); контекстна телеметрія від модулів рішення (атрибути активів), які застосовуються як модифікатори кореляційної логіки.

3.2.1.3 Обробка телеметрії: формати, нормалізація, часові властивості

Підсистема SIEM повинна підтримувати накопичення телеметрії у гетерогенних форматах: текстові журнали, структуровані події, табличні/ключ-значення представлення, специфічні формати виробників засобів захисту. Властивість до підтримки різних джерел у даному контексті трактується як можливість підключати події, що генеруються розподіленими сенсорами та системами, із забезпеченням семантично коректної нормалізації (виділення полів; типізація; уніфікація часових міток; уніфікація ідентифікаторів активів).

Вимогою зумовленою воєнними умовами деградації інфраструктури є підтримка неповної синхронізації. SIEM повинна коректно працювати з подіями, доставленими із запізненням, підтримувати узгодження порядку подій при запізнілому надсиланні подій, зменшувати похибки, спричинені часовими зсувами та неповнотою даних. У технічному проєкті це зафіксовано як вимога до архітектури рішення загалом.

Практично це накладає на SIEM такі архітектурні властивості: наявність інтерфейсу введення даних, що допускає повторні надходження та дублікати; механізми дедуплікації за детермінованими ключами; збереження первинного представлення для подальшого аналізу разом із нормалізованим представленням для пошуку і кореляції, розділення атрибутів часу виникнення та часу надходження як окремих атрибутів, що використовуються в правилах кореляції та в оцінюванні якості спостережності.

3.2.1.4. Кореляція та аналітичні контури, специфічні для задач підвищення спостережності

У розділі 2 показано, що проблемою реагування за умов відключень є зростання невизначеності причин аномалій, які відстежує SOC. Окремі контролі будуються як кореляція подій “відключення електроживлення” з властивостями груп активів, зокрема з часткою динамічних активів, де поріг спрацювання визначається ризик-апетитом та вимогами до спостережності. Відповідно, SIEM повинна підтримувати кореляційні правила, у яких умовами є події безпеки у поєднанні з контекстними ознаками сегмента чи групи активів,

підтримувати параметризацію порогів спрацювань, забезпечувати генерацію результуючої події, яка фіксує факт суттєвої деградації спостережності та використовується аналітиками для адаптації тактики розслідування. SIEM має підтримувати як класичні сигнали про інциденти, але й синтетичні події що свідчать про втрату спостережності, які впливають на трактування інших спрацювань та знижують хибнопозитивні результати.

3.2.1.5. Сховище подій, пошук, інформаційні панелі, керування інцидентами

Як платформа SOC, SIEM повинна забезпечувати зберігання подій і керовані часові горизонти ретенції; індексований пошук і агрегації для аналітичних запитів; візуалізацію у вигляді інформаційних панелей; керування кейсами з фіксацією артефактів розслідування, рішень, часових міток та зв'язків між подіями. У HLD ця роль визначена як “зберігання подій, детекційних правил, інформаційних панелей і керування кейсами”. З огляду на те, що результати підсистем контролів і метрик мають бути представлені в SIEM як інформаційні панелі SOC (метрики; ризикові активи; динамічність/резервування; географічні зрізи), SIEM повинна підтримувати модель візуалізації, придатну для одночасного відображення: станів спостережності (сегментно; по класах критичності); якості телеметрії (простої джерел; затримки надсилання); показників резервування; статистики спрацювань контролів, що пов'язані з відключеннями електроживлення/зв'язку.

3.2.1.6. Вимоги до розподіленого збору та стійкості до деградації зв'язності

Оскільки в технічному проєкті закладено режим неповної синхронізації з буферизацією поза центром мережі, SIEM повинна мати сумісну модель розподіленого збору, а саме: підтримку віддалених колекторів приймання подій; можливість автономного накопичення телеметрії на периферії із подальшою доставкою; контроль цілісності ланцюга доставки .

Важливо зазначити, що відкладене надсилання подій не повинно мати вплив на кореляційні процеси. SIEM повинна підтримувати ретроспективну

кореляцію на певному часовому проміжку, достатньому для типових затримок доставки; повторне обчислення похідних сигналів при надходженні запізнених подій; маркування ступеня повноти даних для інциденту, для врахування факту зменшеної достовірності при подальшому аналізі..

3.2.1.7. Функції безпеки та керованості SIEM як елементу SOC-платформи

SIEM є точкою концентрації телеметрії та прийняття рішень, її архітектурний опис включає контроль доступу та розмежування повноважень; аудит адміністративних дій; політики приймання подій, криптографічний захист каналів та збережених даних, контроль змін правил кореляції. Окремою вимогою щодо керованості є трасованість того, як саме контекстні атрибути SAM і синтетичні події вплинули на спрацювання або приглушення кореляційного правила в SIEM. Підсистема повинна дозволяти відстежувати причини тих чи інших кореляційних результатів у вигляді збережених полів, умов, часових вікон та версій правил.

3.2.1.8. Вихідні результати підсистеми SIEM у межах рішення

SIEM є інтерфейсом перетворення результатів роботи розробленого рішення у операційні артефакти SOC у вигляді сигналів про інциденти. Підсистема реалізує сформовані кореляційні правила з використанням збагачення; синтетичні події, що фіксують стани деградації спостережності та дефіцит резервування; інформаційні панелі метрик для управління рішеннями SOC.

3.2.2. Підсистема активного реагування (EDR, NDR)

Підсистема активного реагування призначена для виконання керованих дій локалізації (стримування) на рівні окремих активів і мережевих сегментів у межах алгоритму декомпозиції системи на керовані компоненти. Її функція — забезпечити цільову ізоляцію компонентів, які можуть бути відокремлені без неприйнятної операційного впливу, та обов'язкову ізоляцію компонентів із підтвердженою нелегітимною/скомпрометованою активністю.

Підсистема спирається на готові продукти як джерела телеметрії та механізми керованого впливу (EDR; NGFW; мережеві засоби) за умови їх наявності.

3.2.2.1. Функціональні вимоги

Підсистема повинна забезпечувати:

1. Виконання ізоляції за рішенням алгоритму декомпозиції; у результаті потрібна підтримка часткової/цільової ізоляції.
2. Технічні механізми мережевої локалізації, спрямовані на мінімізацію міжсегментного поширення шкідливої активності, через EDR/NGFW/мережеві засоби.
3. Відкладену ізоляцію як режим виконання керованих дій у середовищі неповної синхронізації/переривань зв'язку: підсистема має підтримувати буферизацію та повторне виконання команд після відновлення досяжності цільових точок застосування політик. Загальна вимога «відкладеної доставки» і буферизації для рішення задана на рівні HLD.
4. Ізоляцію цілого мережевого сегмента - застосування політик, що припиняють або жорстко обмежують міжсегментну взаємодію (наприклад, між VLAN/зонами довіри), з контролем винятків для критично необхідних сервісів.

3.2.2.2. Інтерфейси та потоки даних

- SIEM - підсистема активного реагування: постановка задач на стримування як частина інциденту; отримання статусів виконання; отримання подій аудиту.
- До EDR: команди ізоляції активу; часткові політики; збір підтверджень виконання та телеметрії.
- До NDR/мережевих засобів/NGFW: політики сегментної ізоляції; мікросегментаційні правила; тимчасові правила маршрутизації/фільтрації; підтвердження застосування.

Підсистема повинна продукувати у SIEM: події «action issued / action applied / action failed / action rolled back»; поля збагачення, що відображають поточний стан ізоляції компонента/активу/сегмента. Вимога доступності результатів у SIEM як подій/полів задана на рівні технічного проєкту.

3.2.2.3. Механізми ізоляції

Ізоляція активу

Переведення активу у режим керованої мережевої взаємодії, в якому дозволені лише канали, необхідні для керування та збору доказів (наприклад, канал керування EDR), а вся інша взаємодія блокується або обмежується політиками. Можлива ізоляція окремої системи, або мережевого сегмента.

Ізоляція окремих функцій

Вибіркове блокування функцій мережевої взаємодії без повної ізоляції; реалізується політиками типу «заборонити lateral movement-вектори» (наприклад, блокування SMB/RDP; обмеження вихідного трафіку; заборона доступу до адміністрування).

Відкладена ізоляція

Режим, у якому рішення про ізоляцію прийняте, але виконання відбувається при настанні умов досяжності та/або працездатності засобів впливу (агент EDR знову в мережі; відновлений канал керування; доступний NGFW контролер тощо).

3.2.3. Підсистема інвентаризації та злиття (SAM Core + Fusion)

3.2.3.1. Призначення та межі підсистеми

Підсистема інвентаризації та злиття призначена для безперервної актуалізації інвентаризації активів у середовищі інтенсивних топологічних змін шляхом багатоджерельного злиття даних (data fusion), з формуванням канонічної моделі активів і позначеного орієнтованого графа залежностей. Межі відповідальності включають SAM Core як ядро моделі, сховищ і сервісних інтерфейсів та Fusion як модуль приймання, нормалізації, розв'язання ідентичностей і конфліктів атрибутів та оцінювання довіри до джерел.

Обчислення похідних атрибутів (зокрема часових атрибутів ідентифікації, геоприналежності, резервування, динамізму, «дескриптора загроз») не належить до цієї підсистеми й виконується окремим модулем атрибутивного профілювання.

3.2.3.2. Роль у логічній архітектурі рішення та вимоги до інтеграції

Підсистема SAM Core + Fusion реалізує базове джерело істини в процесі атрибутивного профілювання, контролів та метрик, забезпечує стабільну ідентифікацію активів і залежностей для подальшого збагачення подій. Вхідні дані мають надходити як спостереження про активи та зв'язки з часовою міткою та обов'язковим збереженням інформації про походження даних. Базовий перелік інтеграцій з джерелами даних залежить від конкретної імплементації, але в рекомендаційному форматі може включати мережевий сканер; систему CMDB; службу каталогів (наприклад, Microsoft Active Directory); CNAPP як джерело інвентаризації хмарних компонентів. Підсистема має надавати API читання/пошуку активів, ідентичностей, атрибутів, графа залежностей і метаданих довіри/свіжості; події змін щодо створення/оновлення активів і зв'язків як тригери для наступних конвеєрів обробки даних.

3.2.3.3. Вхідні дані та конекторний шар Fusion

Fusion повинна реалізовувати конвеєр підключення джерел за схемою «конектор - мапінг - нормалізація - злиття», де додавання нового джерела не змінює SAM Core та не порушує канонічну схему. Конектори мають уніфікувати гетерогенні способи доступу до даних (pull/push) у формат спостережень, забезпечувати формування детермінованих ідемпотентних ключів повідомлень для повторного приймання та фіксувати часові мітки події та надходження як окремі атрибути (для узгодження з режимом неповної синхронізації).

3.2.3.4. Канонічна модель активів у SAM Core

SAM Core повинен містити канонічні сутності та зв'язки: актив; ідентичність активу; атрибут; зв'язок; джерело; журнал змін, а інфраструктура повинна бути подана як позначений орієнтований граф, де вершини відповідають активам, а ребра — відношенням функціональної або мережевої

залежності. Модель активу має підтримувати щонайменше мережеві реквізити (IP-адреси; Fully Qualified Domain Name, FQDN; Virtual Local Area Network, VLAN; MAC-адреси), ознаки платформи (тип/версія операційної системи; склад програмного забезпечення; рівень оновлень), стан покриття засобами захисту, часові метрики інвентаризаційних спостережень та організаційні атрибути (власник; належність до бізнес-системи/сервісу).

3.2.3.5. Нормалізація та семантичне узгодження

Підсистеми повинна забезпечувати приведення атрибутів до канонічних типів і словників, з урахуванням того, що джерела різної природи вимірювання є ортогональними, і використовуються для евристичного підсилення довіри до атрибутів у середовищі. Нормалізація повинна бути трасованою: будь-яке перетворення має зберігати посилання на первинний фрагмент даних джерела через джерело.

3.2.3.6. Розв'язання ідентичностей та конфліктів атрибутів

Fusion повинна реалізовувати зіставлення записів різних джерел в один актив за множиною ключів, зокрема IP-адресою; FQDN; MAC-адресою; серійними ідентифікаторами; ідентифікаторами каталогу; хмарними ідентифікаторами. Для конфліктних значень атрибутів має виконуватись вибір канонічного значення з урахуванням довіри, свіжості та контексту, при цьому альтернативні значення повинні зберігатися як версії з джерелом для ретроспективного аналізу.

3.2.3.7. Побудова та актуалізація графа залежностей

Fusion повинна забезпечувати інкрементальне додавання та уточнення ребер графа залежностей за результатами надходження спостережень, з підтримкою мінімально необхідних типів відношень «залежить від/входить до/розташований у/обслуговує» та збереженням джерела для кожного ребра. Оскільки інвентаризація у воєнний період трактується як безперервна оцінка стану, граф повинен підтримувати часову інтерпретацію: фіксацію моментів появи/зникнення ребер як подій змін.

3.2.3.8. Режим неповної синхронізації та монотонні оновлення

Підсистема повинна підтримувати події з відкладеною доставкою та монотонні оновлення інвентаризаційних даних. Вимога є необхідною для усунення проблеми переривчастої зв'язності та буферизації з подальшим узгодженням. Практично це вимагає ідемпотентної обробки повторів, розмежування атрибутів «часу події» та «часу надходження» в канонічній моделі; можливості повторного запуску інтервалів отримання даних без порушення інваріантів канонічної схеми.

3.2.3.9. Джерела: специфіка мінімально достатнього базису спостереження

Мережевий сканер повинен мати доступ до всіх мережевих сегментів у розподіленій або централізованій архітектурі; його функція — постійне виявлення мережевих активів і їх сервісів та ідентифікація порушень зв'язності між великими сегментами. Служба каталогів (Microsoft Active Directory) повинна використовуватись як шар ідентичностей/облікових записів, що охоплює більшість інфраструктури та забезпечує автоматичну актуалізацію даних керування. CNAPP повинен інтегруватися з панелями керування провайдерів публічних хмарних послуг для збору інвентаризації підключених сервісів/об'єктів та їх конфігурацій; нові хмарні об'єкти мають автоматично долучатися до інвентаризації SAM після появи в домені керування.

3.2.3.10. Вимоги до захищеності та аудиту взаємодій

Міжсистемна взаємодія повинна використовувати комунікації із захистом Transport Layer Security (TLS) з взаємною автентифікацією; доступ до адміністративних і інтеграційних операцій повинен реалізовувати парадигму Role-Based Access Control (RBAC); усі дії та відмови (включно з повторними спробами запису даних та розв'язанням конфліктів) повинні протоколюватися як події, придатні для подальшого аналізу.

3.2.3.11. Вихідні результати підсистеми у межах рішення

Підсистема повинна продукувати канонічний реєстр активів із можливістю пошуку за ключами ідентичності, класом активу, належністю до

сегментів або сервісів та часовими обмеженнями, позначений орієнтований граф залежностей активів, метадані довіри та свіжості атрибутів, зокрема «значення», «джерело», «час», незворотний журнал змін для фактів інвентаризації та рішень злиття; подієвий потік змін активів і зв'язків для ініціювання обчислень у підсистемах атрибутивного профілювання, контролів та метрик, а також для подальшого використання в SIEM через механізми збагачення/синтетичних подій у межах відповідних підсистем.

3.2.4. Модуль обрахунку динамізму

3.2.4.1. Призначення та межі підсистеми

Модуль обрахунку динамізму призначено для формалізованого визначення якісного рівня динамізму активу як міри вразливості спостережності активу до масового відключення електропостачання, з урахуванням того, що втрата живлення первинно зумовлює деградацію доступності активу та/або джерел телеметрії, а також руйнування енергозалежних конфігурацій. У межах рішення модуль виконує лише обчислення, валідацію та версіонування оцінки динамізму для одиничних активів та комплексних активів (система, сервіс, сегмент, майданчик), та формування пояснювальних артефактів і метаданих довіри; отримання первинних атрибутів і топологічних залежностей, а також злиття багатоджерельної інвентаризації належить до підсистеми управління безпековими активами; побудова кореляційних правил, контролів і метрик є функцією окремого модуля контролів.

3.2.4.2. Роль у логічній архітектурі рішення та вимоги до інтеграції

Модуль реалізується як окремий програмний сервіс і працює як споживач даних SAM, використовуючи програмний інтерфейс Application Programming Interface (API) SAM для читання канонічних атрибутів активів, історичних спостережень та графа залежностей. Інтеграційний контракт передбачає можливість запитів: по ідентифікатору активу; по класу активу; по групі (система/сервіс/сегмент); по множині активів, що входять до комплексного активу; по часовому вікну для атрибутів з історією змін. Для результатів модуль

має мати можливість запису в SAM як похідного атрибуту з окремим простором ісен та версією алгоритму, а також генерації події “dynamism_updated” для подальшого використання у підсистемі збору та аналізу подій безпеки SIEM та у підсистемі візуалізації.

3.2.4.3. Вхідні дані з SAM та вимоги до якості даних

Модуль повинен використовувати лише ті ознаки, які можуть бути отримані з SAM без прямої інтеграції з першоджерелами, але з урахуванням метаданих походження та свіжості. Мінімально достатній набір включає: клас активу та роль у системі; наявність/відсутність резервування електроживлення та каналів зв’язку; ознаки енергозалежності конфігурації та/або стану; ознаки волатильності мережевих ідентифікаторів (частота змін IP-адрес/маршрутів/точок підключення); історію досяжності або втрати телеметрії як часові ряди; членство у комплексних активах і залежності в графі. Для кожної ознаки має враховуватися якість даних: джерело; час останнього підтвердження; рівень довіри до джерела, визначений SAM; наявність конфліктних значень, які залишаються збереженими в SAM.

3.2.4.4. Нормалізація ознак та побудова проміжного представлення

Перед застосуванням правил модуль повинен перетворити атрибути SAM у нормалізований вектор ознак, що є інваріантним до різних схем інвентаризації. Нормалізація включає: приведення категоріальних значень до контрольованих словників; перетворення часових рядів у агреговані статистики з фіксованим часовим вікном; визначення бінарних індикаторів відсутності даних як окремих ознак; формування показника “freshness_penalty” як функції давності підтвердження критичних ознак. Проміжне представлення має бути серіалізованим (наприклад, у форматі JSON) і збереженим як частина пояснення результату для відтворюваності.

3.2.4.5. Правила обчислення динамізму для одиничного активу

Оцінка динамізму повинна бути правил-орієнтованою та детермінованою, з можливістю конфігурації без зміни програмного коду. Набір правил має охоплювати принаймні такі причинні механізми: енергозалежність стану або

конфігурації; відсутність або недостатність резервування електроживлення; залежність доступності від проміжної мережевої інфраструктури без резервування; висока частота змін мережевих ідентифікаторів або топології; наявність історичних епізодів втрати телеметрії при підтверджених відключеннях; належність до класів активів, для яких характерна короткоживучість або автоматичне масштабування. Кожне правило повинно формувати внесок у інтегральний числовий бал динамізму у нормованому діапазоні, а кінцеве відображення у якісні рівні “низький/середній/високий” виконується пороговою функцією, параметри якої визначаються політикою організації та ризик-апетитом.

3.2.4.6. Агрегація динамізму для комплексного активу

Для комплексних активів модуль повинен формувати оцінку як функцію розподілу динамізму складових активів та структури залежностей. Підтримуються щонайменше два режими: консервативний, де рівень визначається як максимум серед критичних вузлів графа залежностей; статистичний, де рівень визначається за квантилем або зваженим середнім з вагами, що відображають роль вузлів у забезпеченні спостережності (сенсори, колектори, транспортні компоненти). Правила агрегації повинні враховувати, що втрата невеликої підмножини “вузлів спостереження” може спричинити непропорційне зниження видимості для всієї системи, тому ваги мають бути конфігурованими, а перелік ролей — розширюваним.

3.2.4.7. Планувальник перерахунку та інкрементальна обробка

Модуль повинен підтримувати інцидентний та періодичний режими запуску. Інцидентний режим ініціюється подіями SAM про зміну атрибутів, членства у комплексних активах або залежностей; перерахунок виконується інкрементально для дотичних активів і пов’язаних комплексних активів. Періодичний режим застосовується для контролю дрейфу даних і відновлення узгодженості, коли події могли бути втрачені; частота повинна бути конфігурованою. Повторні запуски повинні бути ідемпотентними, а результати — версіонованими за ідентифікатором конфігурації правил та версією коду.

3.2.4.8. Доказовість, трасованість та контроль якості

Кожен результат повинен містити: якісний рівень; числовий бал; довіру до результату як функцію повноти і свіжості вхідних даних; перелік правил, що спрацювали, з їх внесками; посилання на використані атрибути SAM з часовими мітками; часову мітку обчислення. Модуль повинен підтримувати тестовий набір еталонних профілів активів, на яких валідується стабільність віднесення до класів “низький/середній/високий”, а також механізм виявлення деградації якості даних, коли частка результатів з низькою довірою перевищує поріг.

3.2.4.9. Вихідні результати підсистеми у межах рішення

Модуль повинен формувати та підтримувати в SAM похідні атрибути: “dynamism_level” як якісну класифікацію; “dynamism_score” як нормований бал; “dynamism_confidence” як показник достовірності; “dynamism_explanation” як структурований артефакт відстежуваності; “dynamism_version” як ідентифікатор конфігурації правил і коду. Модуль повинен продукувати події зміни динамізму для передачі відповідних подій у SIEM та відстеження підсистемою візуалізації, щоб забезпечити застосування “фільтра динамізму” у кореляційній логіці та побудову контролів динамічного впливу на спостережність на рівні груп активів.

3.2.5. Модуль обрахунку дескриптора загроз

3.2.5.1. Призначення та межі підсистеми

Модуль обрахунку дескриптора загроз призначено для формування та підтримання дескриптора загроз активу у вигляді формалізованого JSON - атрибуту, що містить релевантні класи загроз з огляду на інфраструктурну роль активу, його експозицію та відображення на тактики і техніки MITRE ATT&CK. Дескриптор загроз визначається як синтетична змінна, що використовується як вхідна для пріоритезації обробки сповіщень, а також для ТН-пріоритезації (Threat Hunting). Механіка ідентифікації дескриптора в межах даного модуля розглядається як зовнішня функція (black box) і не деталізується; модуль відповідає за побудову контексту на основі даних SAM, виклик механізму ідентифікації (детермінованого або з використанням LLM), постпроцесінг,

валідацію, збереження, версіонування та кероване застосування результату в межах рішення. Реалізація модуля виконується мовою програмування Python як окремий сервіс з фіксованим інтеграційним контрактом.

3.2.5.2. Роль у логічній архітектурі рішення та вимоги до інтеграції

Модуль використовує дані підсистеми інвентаризації та злиття даних SAM і використовує її API для отримання канонічної моделі активу, історії спостережень та метаданих походження. Запис результату виконується як похідний атрибут активу у SAM з ізоляцією простору імен, обов'язковою фіксацією версії правил та моделі, часовою міткою обчислення і посиланнями на використані вхідні атрибути. Для інтеграції з підсистемою збору та аналізу подій безпеки SIEM модуль продукує події класу “threat_descriptor_updated” з мінімально достатнім навантаженням для кореляції та пріоритезації, без дублювання чутливих деталей інвентаризації.

3.2.5.3. Вхідні дані з SAM та структурований запис активу

На стадії збору й нормалізації, що передують модулю, виконується автоматизоване злиття даних з мережевих сканерів, CMDB, служб каталогів, систем управління вразливостями та CNAPP у єдину модель активу в SAM. Модуль повинен отримувати з SAM структурований запис, який включає історію змін мережевих реквізитів і стану досяжності; інформацію про рівні резервування електроживлення та зв'язку; часові мітки останньої ідентифікації та останньої успішної ідентифікації; належність до бізнес-сервісу або комплексу; класифікацію за роллю (наприклад, сервер критичного сервісу, робоча станція користувача, елемент технологічної мережі); типові сценарії використання; пов'язані облікові записи та їхні привілеї; ознаки експозиції (відкриті сервіси, межі сегментації, доступність ззовні). Усі атрибути повинні бути доступні разом із джерелом, що уможливорює оцінювання достовірності висновку і керовану деградацію якості при неповних даних [65].

3.2.5.4. Побудова контексту та стандартизоване подання для інтерпретації

На стадії побудови контексту структурований запис перетворюється на стандартизоване текстове або напівструктуроване подання, зокрема придатне для інтерпретації LLM або для застосування еквівалентної детермінованої функції ідентифікації. Контекст повинен містити стислий опис інфраструктурної ролі активу; часовий профіль появи та зникнення в джерелах спостереження; дані про географічне розташування й резервування; перелік основних програмних компонентів і типів інтерфейсів доступу; стислий опис доменів довіри та меж сегментації; ознаки типових каналів початкового доступу та латерального переміщення. Додатково контекст може включати агреговані статистичні показники, зокрема частоту змін атрибутів, частку епізодів недоступності, середню тривалість відмов, а також індикатори експозиції, що підвищують апріорну ймовірність окремих технік [65].

3.2.5.6. Постпроцесінг, формалізація та валідація JSON-атрибуту

На стадії постпроцесінгу відповідь black-box механізму перетворюється на формалізований JSON-атрибут, придатний для автоматизованої обробки. Для дескриптора загроз формується кортеж полів, що включає: перелік технік (ідентифікатори та назви); перелік тактик; ключові вектори атак; очікуваний рівень впливу; агрегований індикатор критичності профілю загроз; показник довіри/якості висновку як функцію повноти та свіжості вхідних даних; раціоналізацію у стислому вигляді; метадані версії (версія правил/моделі, версія схеми JSON); посилання на використані атрибути SAM та довідкові елементи RAG. На цьому етапі накладаються обмеження, що мінімізують варіативність: допустимі значення словників; максимальна кількість технік; заборона вільного тексту поза полями раціоналізації; нормалізація ідентифікаторів MITRE ATT&CK; відсікання некоректних або суперечливих значень із реєстрацією діагностики [65].

3.2.5.7. Вихідні результати підсистеми у межах рішення

Модуль формує та підтримує в SAM похідний атрибут дескриптора загроз у форматі JSON з фіксованою схемою; забезпечує версіонування дескриптора та збереження історії змін; продукує подію “threat_descriptor_updated” для використання у SIEM у функціях пріоритезації сповіщень та ТН-пріоритезації; надає пояснювальний артефакт, що пов’язує техніки MITRE ATT&CK і вектори атак з атрибутами активу та довідковими елементами знань, з оцінкою довіри, придатною для автоматизованого врахування при деградації спостережності.

3.2.6. Підсистема візуалізації та звітності

Підсистема візуалізації та звітності призначена для формалізованого відображення результатів моніторингових контролів і розрахунків показників ефективності на основі даних, що надходять із підсистеми SIEM та з модуля атрибутивного профілювання, контролів та метрик. У межах технічного проєкту вона визначається як підсистема, що забезпечує візуалізацію ефективності роботи рішення та відображення показників і аномалій, пов’язаних зі спостережністю та керованістю реагування.

Архітектурно підсистема реалізує аналітичний контур, відокремлений від операційного контуру кореляції в SIEM. Мета відокремлення полягає у зниженні навантаження на SIEM як платформу подій і управління інцидентами, а також у забезпеченні відтворюваності розрахунків показників у режимах неповної синхронізації, відкладеної доставки подій і монотонних оновлень інвентаризаційних даних, які є базовою умовою функціонування рішення.

3.2.6.1. Джерела даних та інтерфейси інтеграції

Підсистема отримує дані з двох класів джерел. Перший клас складають операційні дані SIEM: агреговані вибірки по подіях, інцидентах і статусах опрацювання; часові характеристики життєвого циклу інцидентів; службові поля збагачення подій, зокрема атрибути активів і синтетичні індикатори втрати спостережності, що формуються іншими підсистемами.

Другий клас представляють результати обчислень модуля атрибутивного профілювання та модуля контролів і метрик: похідні атрибути активів (часи

ідентифікації; історія змін у форматі append-only; географічна приналежність; резервування; динамізм; “дескриптор загроз”); результати правил і метрик (оцінка достатності резервування; профіль загроз; пороги втрати спостережності; пріоритезація threat hunting).

Інтеграційно дані надходять у БД за моделлю періодичної інкрементальної синхронізації з ідемпотентними операціями (тобто повторне завантаження одного й того ж інтервалу не змінює коректного стану). Підсистема реалізує керування інтервалами завантаження, відсічення дублікатів, контроль запізнілих подій, узгодження часових зон та побудову узгодженого “зрізу стану” на момент розрахунку. Умовою коректності є підтримка режиму неповної синхронізації, коли частина подій і оновлень атрибутів може надходити із затримкою.

БД реалізує аналітичну модель у вигляді нормалізованих таблиць та матеріалізованих представлень для швидкого читання. На рівні сутностей доцільно розділяти: факти контролів (кожне спрацювання або вимір із часовою міткою, типом контролю, ключем активу/сегмента, параметрами порогу та результатом); факти інцидентів (ідентифікатори кейсів, стани, часові мітки переходів, причина закриття); довідники активів та їх атрибутів (включно з географічною приналежністю і показниками резервування/динамізму); довідники відповідностей до тактик і технік MITRE ATT&CK® у межах “дескриптора загроз”, оскільки цей атрибут використовується для пріоритезації. Для відтворюваності розрахунків критичні зміни атрибутів і результати контролів фіксуються як події в append-only представленні.

Для прискорення аналітики застосовується партиціювання за часом для великих факт-таблиць; індексація за ключами активу, сегмента та типу контролю; матеріалізація агрегатів для метрик за вікнами часу (година/доба/тиждень) залежно від управлінського горизонту.

3.2.6.2. Оркестрація обчислень і оновлень

Підсистема реалізує формалізований граф завдань (Directed Acyclic Graph, DAG), у якому розділяються етапи: екстракція з SIEM та модулів;

валідація повноти і часової узгодженості; нормалізація схем; збагачення довідниками SAM для забезпечення стабільних ключів активів; розрахунок метрик; публікація агрегованих представлень у БД; протоколювання якості даних (кількість записів; кількість запізнених подій; частка відхилення записів). Відповідність предметній області забезпечується тим, що результати контролів і атрибутів мають бути придатні для побудови інформаційних панелей SOC у частині метрик, ризикових активів, динамічності/резервування та географічних зрізів.

У конвеєрах Підсистеми передбачається відтворюваний розрахунок метрик, зокрема кількості спрацювань системи та відсотку хибнопозитивних спрацювань, як базового критерію ефективності.

3.2.6.3. Візуалізація та звітність

Підсистема забезпечує інтерфейси багатовимірною аналізу та формалізовані панелі показників. На рівні змісту панелі мають відображати: динаміку метрик резервування та порогів втрати спостережності; розподіли “ризикових активів” за атрибутами динамізму, географічної приналежності та рівнів резервування; часові ряди синтетичних подій втрати спостережності та їх співвідношення з операційними показниками опрацювання інцидентів; аналітику пріоритезації threat hunting відповідно до індексу, який включає нормовану критичність та частку покриття релевантних технік MITRE ATT&CK®.

Звітність трактується як відтворювана фіксація стану метрик і контролів за визначений період із контрольованими визначеннями показників. Тому в системі візуалізації мають бути реалізовані: версіонування визначень метрик на рівні SQL-артефактів; шаблони звітів, що посилаються на конкретні представлення у реляційній БД; розмежування доступу (role-based access control) до наборів даних і панелей; журналювання доступів для аудиту використання.

3.2.6.4. Вимоги до надійності та безпеки

Підсистема має зберігати працездатність під час деградації зв'язності шляхом інкрементальної синхронізації, буферизації і повторного запуску інтервалів завантаження, що є необхідним наслідком вимоги підтримки відкладеної доставки та неповної синхронізації. На рівні захисту даних реалізуються мінімізація складу персональних і чутливих даних у аналітичному контурі шляхом псевдонімізації ключів; сегрегація доступів між операційним SIEM та аналітичним БД, контрольована експозиція полів збагачення і атрибутів активів у відповідності до принципу мінімально необхідних привілеїв.

3.3. Прототип технічного рішення

Прототип технічного рішення визначається як мінімально достатня реалізація логічної архітектури, що забезпечує відтворювану перевірку працездатності запропонованих методів підвищення спостережності за умов деградації телеметрії, зокрема в режимі неповної синхронізації (відкладена доставка; монотонні оновлення інвентаризаційних даних; буферизація). Межі прототипу визначаються тим, що він має реалізувати повний наскрізний контур даних «інвентаризація - обчислення похідних атрибутів і метрик - передача результатів у SIEM - підтримка рішень реагування», але допускає використання готових платформних підсистем для збору подій, активного реагування та візуалізації за умови відповідності їх інтерфейсних і функціональних властивостей вимогам HLD.

Прототип орієнтовано на практичну імплементацію прийняття рішень під час реагування в умовах низької спостережності через формування пріоритезованого переліку компонентів для аналізу та застосування керованої ізоляції (повної/часткової/сегментної або відкладеної) залежно від критичності й підтверджень активності загрозового агента

3.3.1. Принципи відкритої архітектури та розмежування «власна розробка / готові компоненти»

Підхід до побудови прототипу характеризується двома критеріями: інтерфейсна заміненість підсистем; семантична узгодженість вихідних

артефактів незалежно від конкретного вендора. У межах технічного проєкту SIEM розглядається як підсистема, в яку результати інших компонентів мають надходити трьома узгодженими способами: як поля збагачення подій для кореляційних правил; як синтетичні події визначених класів («втрата спостережності»; «недостатнє резервування»; «сегментна деградація спостережності»); як інформаційні панелі для оперативного контролю метрик та ризикових зрізів. Формується інваріантний контракт інтеграції, який допускає застосування різних SIEM за умови підтримки відповідних механізмів збору/збагачення/візуалізації.

Підсистема активного реагування розглядається як композиція логічних модулів, незалежних від конкретного технологічного рішення. Підсистема включає службу оркестрації реагування, засіб моніторингу доступності засобів впливу, адаптери інтеграції до зовнішніх програмних інтерфейсів керування; сховище станів дій у форматі append-only. Специфічними до технологічної імплементації є лише механізми примусу та формат команд та телеметрії; керування життєвим циклом дій та аудит є інваріантними.

Розмежування реалізації у прототипі встановлюється так: власною розробкою (програмним кодом) є модулі обчислення похідних атрибутів, які з високою імовірністю не можуть бути налаштовані на рівні конфігурації SIEM або SAM; готовими компонентами є SIEM; EDR/NDR платформа як джерело телеметрії та засіб впливу; підсистема візуалізації та звітності на основі окремого стеку; конкретний перелік компонентів, що мінімально мають бути реалізовані власними силами, зафіксовано в технічному проєкті.

3.3.2. Апробаційний технологічний стек прототипу та обґрунтування вибору

У прототипі як апробаційні компоненти застосовано: Elasticsearch+Logstash+Kibana [69] як реалізацію підсистеми збору та аналізу подій/інцидентів; PostgreSQL та власні програмні модулі як система інвентаризації активів у підсистемі SAM Core + Fusion; PostgreSQL як транзакційно-аналітичне сховище (канонічні сутності; підтримка відстеження

джерел; часові ряди метрик; журнали дій); Kibana як реалізація підсистеми візуалізації та звітності.

Вибір Python як базової мови для власної розробки зумовлено вимогами прототипу до: швидкої ітерації моделей даних та алгоритмів; наявності зрілої екосистеми бібліотек для інтеграцій (HTTP-клієнти; авторизаційні механізми; підписи); підтримки детермінованих обчислень з відтворюваністю; підтримки асинхронної взаємодії з багатьма джерелами телеметрії та керованих дій. На рівні наукової відтворюваності критичною є можливість формалізувати «вхідний стан - параметри ризик-апетиту - вихідні атрибути/метрики» як детерміноване відображення та фіксувати версії вхідних станів [70].

Вибір PostgreSQL обґрунтовано як компроміс між транзакційною узгодженістю (для канонічних сутностей активів і журналів змін append-only) та аналітичною придатністю.

3.3.3.1. Модулі обрахунку динамізму та дескриптора загроз

Було розроблено мінімально-достатній прототип Python-коду модулю обрахунку динамізму активів. Модуль отримує канонічні атрибути з підсистеми керування безпековими активами SAM через API, записує похідні атрибути `dynamism_*` та публікує подію `dynamism_updated`.

Модуль обрахунку дескриптора загроз формує формалізований атрибут у форматі JSON з відображенням на MITRE ATT&CK®, працює як споживач SAM через API, записує результат як похідний атрибут і публікує подію `threat_descriptor_updated`.

Програмний код наводиться в Додатку Б.

3.3.4. Внутрішні потоки даних і сценарій роботи прототипу

Наскрізний workflow прототипу визначається як послідовність відтворюваних операцій збирання, зберігання, обчислення та публікації даних між трьома основними технологічними компонентами: Elastic Stack / ELK (Elasticsearch, Logstash/Kibana, у межах експерименту — Elastic Security як реалізація SIEM, PostgreSQL як сховищем SAM і Python-модулями обчислення

похідних атрибутів. На відміну від цільової архітектури, де оркестрація може виконуватись окремим планувальником конвеєрів, у лабораторному прототипі workflow реалізовано спрощено: через пакетні Python-скрипти, завантаження підготовлених подій у ELK, оновлення таблиць PostgreSQL та подальшу перевірку результатів правилами кореляції і запитами до експериментальних таблиць.

Логічно розрізняються три потоки даних: інвентаризаційний; контекстно-аналітичний; реактивно-кореляційний. Таке розділення відповідає функціональному поділу між реєстром активів, модулем атрибутивного профілювання та підсистемою подієвої аналітики. У межах експерименту кожен потік має фіксовані вхідні артефакти, відтворювані правила перетворення та контрольовані вихідні ознаки, що дозволяє порівнювати базовий режим і пропонований режим без зміни складу початкових сценаріїв.

Інвентаризаційний потік починається з ініціалізації PostgreSQL-схеми підсистеми SAM. У таблиці `sam_assets` фіксується канонічний стан активів: клас активу, роль, сегмент, сервісна група, критичність, географічна приналежність, резервування електроживлення, резервування каналу зв'язку, наявність хмарного агента, можливості реагування, часові атрибути останнього спостереження та похідні поля для подальших обчислень. Модель замінює у прототипі повноцінне багатоджерельне злиття даних з CMDB, Active Directory, мережевих сканерів або Cloud-Native Application Protection Platform (CNAPP), але зберігає необхідну семантику SAM: актив розглядається як об'єкт з технічними, часовими, топологічними й безпековими атрибутами.

У межах прототипу джерелом інвентаризаційних даних є підготовлений набір синтетичних активів, завантажений у PostgreSQL. Цей набір відображає розподілену інфраструктуру з декількома сегментами, локаціями центрів обробки даних та edge-локаціями, серверами застосунків, контролерами домену, мережевими пристроями, робочими станціями, сегментними маяками та засобами безпеки. Для забезпечення відтворюваності первинний стан SAM

фіксується до запуску сценаріїв, а обчислені атрибути записуються назад у ті самі або пов'язані таблиці як результат роботи Python-модулів.

Контекстно-аналітичний потік реалізується Python-кодом, який читає канонічні атрибути активів із PostgreSQL, нормалізує їх і обчислює похідні показники. До таких показників належать оцінка динамізму активу, дескриптор загроз, індекс пріоритезації Threat Hunting і оцінка втрати спостережності. Оцінка динамізму визначає чутливість активу до втрати електроживлення, каналу зв'язку або топологічної зміни; дескриптор загроз формує зв'язок між роллю активу, його експозицією та релевантними тактиками і техніками MITRE ATT&CK; індекс ТН використовується для ранжування активів, щодо яких доцільна поглиблена перевірка.

Результат контекстно-аналітичного потоку має два способи використання. Перший спосіб — оновлення SAM-записів у PostgreSQL, що забезпечує наявність актуального атрибутивного стану для подальших SQL-запитів, агрегацій і розрахунку експериментальних метрик. Другий спосіб — передавання контексту до SIEM-рівня у формі полів збагачення або синтетичних подій. У прототипі це подано через структуру подій, що надходять до Elasticsearch: кожна подія містить не лише факт недоступності, зміни стану або логічної аномалії, а й контекст активу — `asset_name`, `segment_id`, `role`, `criticality`, `geo_affiliation`, `power_backup_minutes`, `channel_backup_minutes`, `cloud_agent_present` та службові ознаки кореляції.

Реактивно-кореляційний потік виконується на рівні ELK. Підготовлені події експериментальних сценаріїв імітують телеметрію від SAM-модуля, сенсорів доступності, контролів логування, каналів зв'язку, сегментних маяків і засобів безпеки. Події завантажуються до Elasticsearch, після чого правила Elastic Security або запити до індексів подій оцінюють наявність характерних профілів: масова втрата спостережності внаслідок відключення електроживлення; деградація каналу зв'язку без підтвердженого power-outage-контексту; відновлення після деградації; зловмисна активність, замаскована під масове технічне відключення.

У proposed-режимі кореляція не обмежується послідовністю технічних подій `asset_unreachable`, `last_log_gap_detected` або `segment_beacon_missing`. Вона використовує контекст SAM: географічну приналежність активів, належність до сегменту, резервування електроживлення і зв'язку, критичність, динамізм та ознаки керованості реагування.

Результатом реактивно-кореляційного потоку є формування синтетичних станів спостережності, що можуть бути подані в ELK як окремі події або як сигнали кореляційних правил. До таких станів належать `synthetic_loss_of_visibility`, `synthetic_segment_visibility_degradation`, `synthetic_insufficient_redundancy`, `synthetic_threat_hunting_priority_changed` і `synthetic_response_capability_state`. У базовому режимі аналогічні події недоступності обробляються без повного SAM-контексту, що створює більшу кількість хибнопозитивних або невизначених інтерпретацій.

Експериментальний workflow завершується фіксацією результатів у PostgreSQL. Таблиці експериментального контуру зберігають сценарії, прогони, режим виконання, еталонні класи подій, спрацювання правил і підсумкові метрики. Забезпечується порівнюється базовий і пропонуваній за часткою хибнопозитивних спрацювань, кількістю пропущених станів, точністю класифікації причин втрати спостережності, а також за здатністю системи відокремлювати інфраструктурну деградацію від накладеної зловмисної активності.

3.3.5. Підсистема візуалізації та звітності в прототипі

Підсистема візуалізації та звітності в лабораторному прототипі реалізується двома взаємодоповнювальними засобами: Kibana як інтерфейс аналізу подій і сигналів ELK та SQL-запити до PostgreSQL як механізм відтворюваного розрахунку експериментальних метрик. У прототипі основний акцент перенесено на мінімальну кількість компонентів і пряму перевірку гіпотези щодо впливу SAM-контексту на якість кореляції.

Kibana використовується для аналізу подій: перегляду часових рядів недоступності активів, сегментної деградації, втрати каналів зв'язку,

повернення активів після відновлення, а також для аналізу синтетичних подій proposed-рішення. Інформаційні панелі в Kibana групують події за сценарієм, сегментом, географічною приналежністю, типом активу, роллю, критичністю та кореляційними ознаками. Окремо відображаються події, у яких застосовано power-outage-контекст, channel-degradation-контекст або ознаки зловмисного накладення зловмисної активності.

PostgreSQL використовується для аналітичної звітності, пов'язаної з активами, атрибутами та результатами експерименту. SQL-представлення або запити формують зрізи за рівнем динамізму, достатністю резервування, розподілом критичних активів за сегментами, наявністю можливостей реагування, індексом ТН та оцінкою втрати спостережності. Однаковий початковий набір активів, однаковий набір сценарних подій і однакова версія Python-алгоритму мають давати однакові значення метрик.

Звітність у прототипі визначається як фіксація результатів кожного запуску експериментального сценарію. Кожен результат прив'язаний до сценарію, режиму виконання, часового інтервалу, версії набору подій і версії алгоритму обчислення похідних атрибутів. Основними звітними зрізами є: кількість подій втрати спостережності за сегментами; частка активів із недостатнім резервуванням; кількість синтетичних подій за типами; відповідність кореляційного результату еталонному сценарію; кількість хибнопозитивних інтерпретацій у базовому режимі; кількість коректно класифікованих станів у proposed; перелік активів із високим індексом ТН; активи, для яких можливість реагування обмежена через втрату керованості EDR або мережових засобів впливу.

Висновки до розділу

На основі проведеного дослідження розроблено вимоги та архітектуру технічного рішення покращення спостережності комп'ютерної системи, що імплементує розроблені методи. Завдання вирішено шляхом формування високорівневого проєкту, у якому визначено призначення, межі, функціональний склад, вимоги до даних, інтеграційні контракти та правила

взаємодії між підсистемами. Архітектура побудована як відкрита модульна система, що включає підсистему збору та аналізу подій безпеки на основі системи управління подіями та інцидентами безпеки, підсистему активного реагування на основі засобів захисту кінцевих точок та мережі, підсистему інвентаризації та злиття даних, модуль обрахунку динамізму, модуль визначення дескриптора загроз, підсистему контролів, а також підсистему візуалізації та звітності. Визначено розподіл між готовими технологічними компонентами та власною розробкою: усі компоненти, окрім підсистеми інвентаризації, модулів обчислення динамізму та дескриптора загроз, механізмів збагачення подій, та логіки підтримки реагування визначені як варіативна частина запропонованого рішення. Результатом виконання завдання є архітектурна декомпозиція, яка забезпечує практичну імплементацію методів розділу 2 без прив'язки до конкретного виробника та екземпляра технічного компонента та дозволяє імплементувати методологію в операційні процеси системи управління подіями та інцидентами безпеки.

РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ СИСТЕМИ СПОСТЕРЕЖНОСТІ ІКС ТА ЗМЕНШЕННЯ НЕВИЗНАЧЕНОСТІ У ВИЯВЛЕННІ КІБЕРІНЦИДЕНТІВ

Експериментальна перевірка спрямована на підтвердження технічної спроможності та вимірюваної ефективності розробленої методології – за допомогою визначених методів виконується багатоджерельна ідентифікація втрати спостережності та диференціація її причин та динамічна сегрегація і пріоритезація високоризикових подій в умовах обмеженої спостережності. Перевірка спирається на визначену логічну модель рішення, у якій SIEM виконує функцію платформи кореляції подій, зберігання подій, детекційних правил, візуалізації та керування інцидентами, тоді як модулі обрахунку динамізму і дескриптора загроз реалізуються власними програмними засобами поверх інвентаризаційної підсистеми SAM.

4.1. Мета та логіка експерименту

Метою експерименту є кількісне підтвердження того, що використання запропонованої методології дозволяє зменшити невизначеність під час аналізу масових подій втрати доступності, знизити частку хибнопозитивних рішень, зменшити ризик хибнонегативного пропуску реальної атаки на тлі деградації електроживлення або зв'язку, а також скоротити часові витрати на первинну інтерпретацію інцидентів. Оцінка результату роботи системи проводиться за кількісним принципом, на основі значення метрик SOC-CMM, а саме відносної кількості хибнопозитивних спрацювань, часу виявлення та пріоритизації задач.

Робоча гіпотеза експерименту полягає в тому, що поєднання контекстних подій спостережності, кореляції альтернативних індикаторів втрати живлення або зв'язку, фільтра динамізму та атрибуту дескриптора загроз приводить до статистично значущого поліпшення принаймні частини ключових операційних метрик SOC-CMM порівняно з базовим режимом кореляції, в якому такі контекстні механізми відсутні. Як базовий критерій ефективності приймається скорочення середнього часу виявлення Mean Time to Detect (MTTD) для інцидентів, пов'язаних з аваріями або відключеннями електропостачання, а

також поліпшення пов'язаних похідних метрик: Percentage of False Positives, Number of False Negatives.

4.2. Методи оцінки результатів експерименту

З метою кількісної оцінки результатів роботи системи під час експерименту невід'ємною частиною процесу є побудова спеціалізованих інформаційних панелей, що фіксують проміжні та кінцеві результати кожного сценарію.

Одним з завдань експерименту є створення інформаційних панелей Observability State (відображає кількість синтетичних подій зникнення спостережності системи та сегменту, часові ряди втрат та розподіл по сегментах), Baseline vs Proposed (пряме зіставлення кількості спрацювань за сценаріями й режимами), Cause Differentiation (розподіл observability.cause та таймлайни для окремих сегментів, що дозволяє верифікувати відсутність змішування power_outage, network_degradation і malicious_activity), Dynamicity, Threat Descriptor / TH Prioritization, Redundancy and Response Capability, кожний з яких пов'язаний із відповідною дослідною гіпотезою.

Інформаційні панелі мають візуалізувати та забезпечити доказовість результатів експерименту.

4.3. Експериментальний стенд

Для забезпечення відтворюваності, мінімізації підготовчих витрат та обмеження складу технічних засобів в ході експерименту застосовано лабораторний стенд мінімальної конфігурації, що відтворює ключові функції цільової архітектури. До його складу входять: платформа ELK (Elasticsearch, Logstash, Kibana) як реалізація SIEM; реляційна база даних PostgreSQL для зберігання інвентаризаційних атрибутів SAM та проміжних результатів обробки; програмний генератор подій на Python на основі утиліти з відкритим кодом FluentBit; програмні модулі обрахунку динамізму, дескриптора загроз та формування контекстних подій спостережності; набір тестових активів та їх програмних моделей, достатніх для породження подій різних типів. Додаткові спеціалізовані продукти, окрім ELK, PostgreSQL та Python-компонентів, у

межах даного експерименту не є обов'язковими. В рамках відтворення концепції можливо використання інших програмних рішень в якості SIEM та SAM.

У межах стенда ELK використовується як кореляційна підсистема, що приймає первинну телеметрію та контекстні події, виконує правила кореляції, формує сповіщення і синтетичні події, а також надає інструментарій для візуального підтвердження результатів у вигляді журналів, інформаційних панелей. PostgreSQL виконує функцію зберігання канонічного представлення активів і їх атрибутів: класу активу, критичності, належності до сегмента, рівня резервування електроживлення і зв'язку, географічної приналежності, часових атрибутів актуальності, рівня динамізму та дескриптора загроз. Ці атрибути, відповідно до HLD-опису рішення, мають бути доступні для збагачення подій у SIEM і використання в правилах кореляції. Архітектура тестового стенду представлена на рис.6., на рис.7 відображено структуру таблиць та зв'язки між даними у стенді.

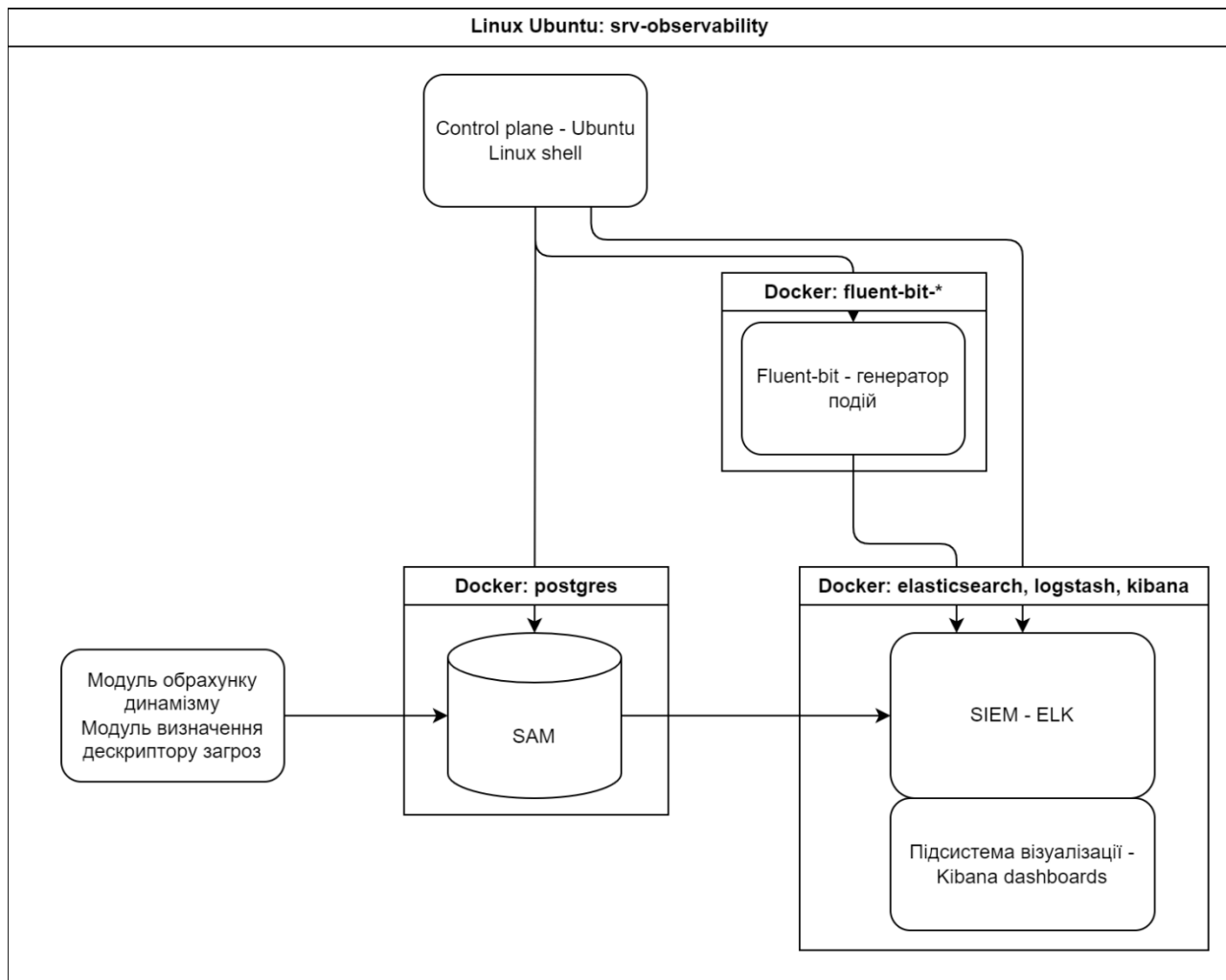


Рисунок 6 - Архітектура тестового стенду

Таблиця 7 - Перелік компонентів тестового стенду

Компонент	Тип	Версія/джерело
srv-observability	Ubuntu Linux Virtual Machine	Ubuntu 24.04.4 LTS
postgres	Docker container	postgres:16
kibana	Docker container	kibana:9.3.1
logstash	Docker container	logstash:9.3.1
elasticsearch	Docker container	elasticsearch:9.3.1
fluent-bit-baseline	Docker container	FluentBit:4.2.3
fluent-bit-proposed	Docker container	FluentBit:4.2.3
Модуль обрахунку динамізму	Python module	v 1.0 – Додаток Б

Модуль дескриптору загроз	визначення	Python module	v 1.0 – Додаток Б
------------------------------	------------	---------------	-------------------

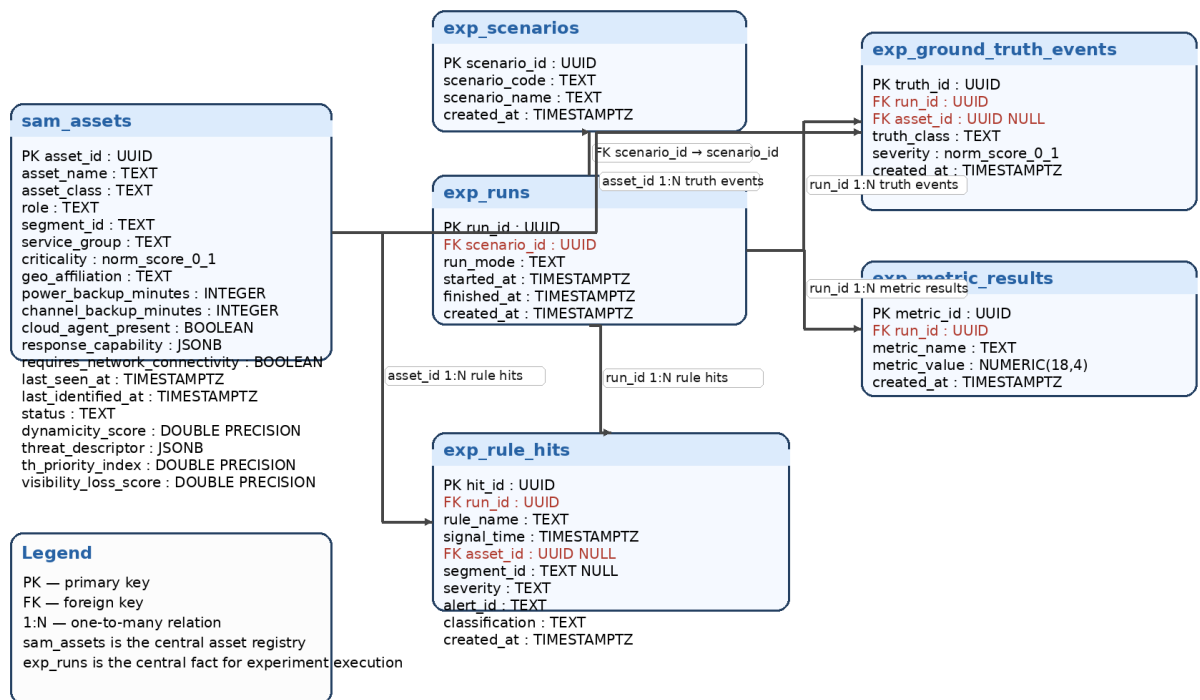


Рисунок 7 - Схема таблиц, що використовується в PostgreSQL SAM

4.3. Дані та моделі, використані в експерименті

Експеримент спирається на спрощену, але семантично повну модель активу. Кожний актив у SAM подається як об'єкт з набором атрибутів, достатніх для побудови контекстно-орієнтованих контролів у SIEM. До обов'язкових атрибутів належать: унікальний ідентифікатор, мережеві реквізити, тип активу, належність до сегмента, рівень критичності, атрибути резервування електроживлення і резервування зв'язку, географічна приналежність, часові атрибути останньої успішної ідентифікації, наявність засобів захисту або керованого реагування, рівень динамізму та дескриптор загроз.

Дескриптор загроз в межах експерименту задається як синтетичний структурований атрибут, пов'язаний з інфраструктурною роллю активу, його експозицією відображенням на техніках MITRE ATT&CK. У межах цього експерименту механізм побудови дескриптора спрощено до детермінованого Python-алгоритму, що формує значення на основі типу активу, його сегмента та експозиції.

В рамках експерименту моделюється робота з реальною інформаційною інфраструктурою організації, що складається з 25 систем, що мають різні сегменти, характеристики, спроможності щодо реагування на інциденти кібербезпеки. Набір даних сформовано на основі експертної оцінки, відштовхуючись від вимог відображення різноманітної, але реалістичної інфраструктури з різними параметрами резервування та критичності. Набір даних, що використовувався для моделювання переліку систем інфраструктури викладено.

4.4. Обмеження експерименту

Запропонований експеримент не претендує на повне відтворення масштабу реальної корпоративної чи державної інфраструктури та не моделює повністю всі класи телеметрії, характерні для продуктивного SOC та всі методи, які застосовуються для покращення спостережності в військових умовах. Його призначення полягає в підтвердженні принципової технічної реалізованості запропонованих методів, відтворюваність їх логіки у кореляційній платформі ELK та наявність вимірюваного позитивного ефекту за ключовими метриками аналізу і реагування. За рахунок такої постановки забезпечується баланс між науковою коректністю, відтворюваністю та обмеженнями практичного часу на підготовку і проведення експерименту.

4.5. Підготовка експерименту

Початковим етапом підготовки було формування робочого каталогу експерименту та впорядкування артефактів. У межах хост-системи створювався окремий каталог, до якого було винесено SQL-схему бази даних, початковий набір активів, Python-модулі, а також чотири набори сценарних подій. Паралельно визначались змінні середовища для доступу до Elasticsearch, Kibana, PostgreSQL та контейнера FluentBit. Це рішення було критичним для забезпечення відтворюваності: усі подальші кроки — ініціалізація БД, імпорт інвентаризації, обчислення атрибутів, експорт довідкового індексу SAM, формування двох потоків подій — спиралися на єдину файлову та контейнерну структуру.

Після створення базового контейнерного контуру було виконано ініціалізацію PostgreSQL схемою експерименту (рис.8, рис.9). SQL-схема передбачала, з одного боку, таблицю sam_assets як канонічний реєстр активів з похідними атрибутами спостережності й пріоритезації, а з іншого — експериментальні таблиці exp_scenarios, exp_runs, exp_ground_truth_events, exp_metric_results, exp_rule_hits, необхідні для фіксації сценаріїв, прогонів, ground truth та результатів оцінювання. Важливо, що в схемі sam_assets атрибут threat_descriptor був визначений як JSONB NOT NULL DEFAULT '{}':jsonb, стенд відразу проєктувався як середовище, де дескриптор загроз є обов’язковим елементом моделі активу, а не факультативним доповненням. Після створення схеми було виконано завантаження стартового набору активів.

```
admin@srv-observability: /02_EXPERIMENT/artifacts$ sudo docker exec -e PGPASSWORD="$PG_PASS" -i "$PG_CONT" psql -U "$PG_USER" -d "$PG_DB" -c "\dt"
```

Schema	Name	Type	Owner
public	assets	table	cmdb_user
public	exp_ground_truth_events	table	cmdb_user
public	exp_metric_results	table	cmdb_user
public	exp_rule_hits	table	cmdb_user
public	exp_runs	table	cmdb_user
public	exp_scenarios	table	cmdb_user
public	sam_assets	table	cmdb_user
public	services	table	cmdb_user

(8 rows)

Рисунок 8 - Демонстрація структури таблиць PostgreSQL в рамках тестового стенду.

```
admin@srv-observability: $ sudo docker exec -e PGPASSWORD="$PG_PASS" -i "$PG_CONT" psql -U "$PG_USER" -d "$PG_DB" -c "SELECT asset_name, segment_id, criticality, power_backup_minutes, channel_backup_minutes FROM sam_assets ORDER BY asset_name;"
```

asset_name	segment_id	criticality	power_backup_minutes	channel_backup_minutes
asp01.coal.lab	SEG-C	0.8800	0	30
asp02.coal.lab	SEG-B	0.9400	0	30
db01.coal.lab	SEG-B	0.9500	180	120
db02.coal.lab	SEG-C	0.9100	0	45
dc01.coal.lab	SEG-A	0.9800	240	180
dc02.coal.lab	SEG-B	0.9700	240	180
edr-sensor01.coal.lab	SEG-A	0.8700	45	90
edr-sensor02.coal.lab	SEG-B	0.8600	45	90
filesrv01.coal.lab	SEG-B	0.8500	60	60
jump01.coal.lab	SEG-A	0.9200	120	120
router01.coal.lab	SEG-A	0.9300	90	180
router02.coal.lab	SEG-B	0.9000	90	180
segbeacon01.coal.lab	SEG-A	0.7400	30	60
segbeacon02.coal.lab	SEG-B	0.7400	30	60
segbeacon03.coal.lab	SEG-C	0.7400	0	60
switch01.coal.lab	SEG-A	0.7800	0	0
switch02.coal.lab	SEG-B	0.7700	0	0
switch03.coal.lab	SEG-C	0.7600	0	0
web01.coal.lab	SEG-A	0.8300	0	60
web02.coal.lab	SEG-C	0.8200	0	60
ws001.coal.lab	SEG-A	0.4200	0	15
ws002.coal.lab	SEG-A	0.4100	0	15
ws003.coal.lab	SEG-B	0.4000	0	15
ws004.coal.lab	SEG-B	0.3900	0	15
ws005.coal.lab	SEG-C	0.3800	0	15
ws006.coal.lab	SEG-C	0.3700	0	15

(26 rows)

Рисунок 9 - Демонстрація наповнення таблиць PostgreSQL тестовими даними.

4.6. Сценарії експериментальної перевірки

Для верифікації методів використовується сукупність сценаріїв, що відтворюють типові для воєнного середовища ситуації деградації спостережності. Сценарії розроблені на основі емпіричного досвіду взаємодії з інфраструктурами в умовах впливів військових умов, аналізі статистичних показників викладених у Розділі 1 та екстраполяції моделей порушення спостережності.

Перший сценарій моделює масову втрату електроживлення без наявності шкідливої активності. У межах визначеного сегмента або групи активів припиняється надсилання телеметрії, генеруються події завершення роботи, перезапусків, затриманого відновлення агентів і тимчасових змін ідентифікаційних ознак. Очікувано, у базовому режимі кореляції така сукупність подій породжує надлишкову кількість спрацювань щодо компрометації або відмови окремих засобів захисту. В експериментальному режимі має формуватися синтетична подія підтвердженої втрати спостережності сегмента, а частина пов'язаних сигналів повинна приглушуватися або знижувати пріоритет на підставі контексту.

Другий сценарій моделює дійсну шкідливу активність на тлі підтвердженого відключення живлення або деградації сегмента. На фоні масової втрати доступності генеруються ознаки, що не пояснюються профілем легітимного відключення електропостачання, а саме - локальне очищення журналів, несанкціонована зміна конфігурації, атипове зникнення телеметрії лише в частині критичних систем або спроба прихованого вимкнення засобу захисту. У цьому випадку контролі, налаштовані в експериментальному режимі не мають помилково інтерпретувати всі симптоми як побічні ефекти екзогенного впливу, а завдяки дескриптору загроз і фільтру динамізму зберегти підвищений пріоритет для активів, чий профіль загроз або експозиція робить компрометацію більш імовірною. Цей сценарій слугує для підтвердження того, що зниження концентрації хибнопозитивних сигналів не досягається ціною зростання хибнонегативних пропусків.

Третій сценарій моделює деградацію каналу зв'язку без втрати електроживлення. У цьому випадку частина телеметрії не досягає SIEM за відсутності артефактів вимкнення електропостачання, а наявність окремих альтернативних ознак свідчить про збереження працездатності активів. Метою сценарію є перевірка спроможності методу багатоджерельної ідентифікації втрати спостережності коректно диференціювати втрату зв'язку, втрату електроживлення та ознаки потенційно навмисного приховування активності.

Четвертий сценарій відтворює фазу відновлення після переривання живлення, коли в інфраструктурі масово спостерігаються перезавпуски, відкладене надсилення журналів, зміни конфігураційних атрибутів і тимчасова нестабільність сервісів. В цій фазі має проявлятися ефект фільтра динамізму, оскільки для високодинамічних активів частина аномалій є очікуваною, а для низькодинамічних — навпаки, потребує окремої перевірки. [71] [72] [73] [74] [75] [76]

Усі сценарії були оформлені у вигляді потоків подій ndjson та використовувались для передачі в SIEM через FluentBit.

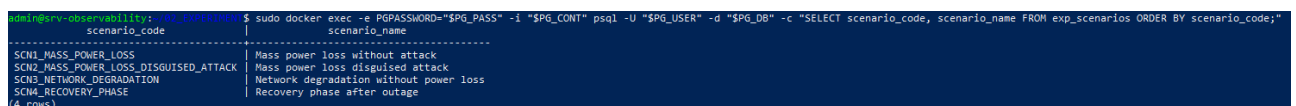
Узагальнено сценарії подаються в таблиці 8.

Таблиця 8 - перелік сценаріїв тестування системи

Сценарій	Дані, використані в тестуванні
SCN1 — Масова втрата електроживлення без атаки	завантажено сирих подій: 142; кількість сегментів у сценарії: 2; сегмент SEG-KYIV-DC: 7 assets; сегмент SEG-LVIV-BRANCH: 5 assets; загальна кількість уражених активів: 12; причина: відключення електроживлення.
SCN2 — Масова втрата електроживлення, замаскована під атаку	завантажено сирих подій: 167; кількість сегментів у сценарії: 2; сегмент SEG-KYIV-DC: 6 assets; сегмент SEG-LVIV-BRANCH: 4 assets; загальна кількість уражених активів: 10; причина: відключення електроживлення з накладенням зловмисної активності.
SCN3 — Деградація каналу зв'язку без втрати живлення	завантажено сирих подій: 119; кількість сегментів у сценарії: 2; сегмент SEG-KYIV-DC: 5 assets; сегмент SEG-ODESA-BRANCH: 4 assets; загальна кількість уражених активів: 9; причина: деградація каналу зв'язку.
SCN4 — Фаза відновлення після outage	завантажено сирих подій: 154; кількість сегментів у сценарії: 2; сегмент SEG-KYIV-DC: 7 assets; сегмент SEG-LVIV-BRANCH: 5 assets; загальна кількість уражених активів: 12; причина: фаза відновлення.

Усього / середнє по 4 сценаріях	усього завантажено сирих подій: 582; кількість сценаріїв: 4; кількість екземплярів сегментів: 8; загальна кількість уражених активів: 43; кількість активів у вибірці для оцінки динамізму: 8
---------------------------------	---

Щоб забезпечити експериментальну відтворюваність, після завантаження активів у БД було створено службові записи сценаріїв і прогонів (рис.10). У таблицю `exp_scenarios` заносились чотири сценарії: масова втрата електроживлення без атаки, масова втрата електроживлення із маскуванням атаки, деградація каналу зв'язку без втрати живлення та `recovery`-фаза після відновлення. Для кожного сценарію в `exp_runs` одразу створювались два запуски — базовий (`baseline`) і пропонуванний (`proposed`).



```

admin@srv-observability: ~$ sudo docker exec -e PGPASSWORD="$PG_PASS" -i "$PG_CONT" psql -U "$PG_USER" -d "$PG_DB" -c "SELECT scenario_code, scenario_name FROM exp_scenarios ORDER BY scenario_code;"
 scenario_code | scenario_name
-----
 SC01_MASS_POWER_LOSS | Mass power loss without attack
 SC02_MASS_POWER_LOSS_DISGUISED_ATTACK | Mass power loss disguised attack
 SC03_NETWORK_DEGRADATION | Network degradation without power loss
 SC04_RECOVERY_PHASE | Recovery phase after outage
(4 rows)

```

Рисунок 10 - демонстрація наповнення таблиць PostgreSQL сценаріями, запланованими для експериментального дослідження.

4.7. Метрики та порядок оцінювання

Після створення стартового SAM-зрізу було виконано обчислення похідних атрибутів активів за допомогою модуля `sam_fusion_func.py` — реалізація модулів обрахунку динамізму та визначення дескриптора загроз (рис.11). У ньому функція `compute_and_update_dynamicity()` обчислювала та записувала для всіх активів `dynamicity_score` і `visibility_loss_score`, а функція `compute_and_update_threat_descriptor()` — `threat_descriptor` і `th_priority_index`.

Цей етап був принциповим для всього експерименту, оскільки в запропонованому режимі кореляційна логіка повинна була працювати не лише з стандартними подіями про недоступність, а й з інформацією про динамізм активу, його пріоритет для загрозового пошуку, резервування та наявні технічні спроможності реагування. Без попереднього заповнення таких атрибутів будь-яке зіставлення базового і пропонуваного режимів втрачало б предметний зміст.

```
(.venv) admin@srv-observability:~/02_EXPERIMENT/artifacts$ python - <<'PY'
> import pycpg2
> from sam_fusion_func import compute_and_update_dynamicity, compute_and_update_threat_descriptor
>
> conn = pycpg2.connect(
>     host="127.0.0.1",
>     port=5432,
>     dbname="cddb",
>     user="cddb_user",
>     password="KnowTheWay",
> )
>
> try:
>     print("dynamicity updated:", compute_and_update_dynamicity(conn))
>     print("threat descriptor updated:", compute_and_update_threat_descriptor(conn))
> )
PY> finally:
>     conn.close()
> PY
dynamicity updated: 26
threat descriptor updated: 26
```

Рисунок 11 - процес збагачення тестових даних PostgreSQL даними SAM Fusion з використанням python.

Після запуску модуля результати ідентифікації динамізму та дескриптора загроз відображено у БД (рис.12).

```
(.venv) admin@srv-observability:~/02_EXPERIMENT/artifacts$ sudo docker exec -e PGPASSWORD="$PG_PASS" -i "$PG_CONTAINER"
atio' AS observable_coverage_ratio FROM sam_assets ORDER BY th_priority_index DESC NULLS LAST;"
asset_name | dynamicity_score | visibility_loss_score | th_priority_index | observable_coverage_ratio
```

dc01.coal.lab	0.19	0.133	0.8105	0.85
db02.coal.lab	0.6075	0.65025	0.80475	0.525
dc02.coal.lab	0.19	0.133	0.8045	0.85
db01.coal.lab	0.19	0.133	0.7925	0.6
router01.coal.lab	0.53	0.421	0.783	1.0
jump01.coal.lab	0.343333	0.273667	0.777	1.0
app01.coal.lab	0.735	0.7645	0.7655	0.75
router02.coal.lab	0.53	0.421	0.765	1.0
edr-sensor01.coal.lab	0.515	0.4855	0.7495	0.4
web02.coal.lab	0.68	0.676	0.7495	0.95
switch03.coal.lab	0.89	0.923	0.7485	0.3
edr-sensor02.coal.lab	0.515	0.4855	0.7435	0.4
switch01.coal.lab	0.89	0.923	0.7355	0.3
web01.coal.lab	0.68	0.676	0.7305	0.95
switch02.coal.lab	0.89	0.923	0.7295	0.3
app02.coal.lab	0.735	0.7645	0.7165	0.75
segbeacon03.coal.lab	0.78	0.746	0.689	0.45
filesrv01.coal.lab	0.486667	0.507333	0.6825	0.85
segbeacon02.coal.lab	0.733333	0.696667	0.6565	0.5
segbeacon01.coal.lab	0.733333	0.696667	0.6565	0.5
ws001.coal.lab	0.8525	0.87175	0.44325	0.725
ws002.coal.lab	0.8525	0.87175	0.43725	0.725
ws003.coal.lab	0.8525	0.87175	0.43125	0.725
ws004.coal.lab	0.8525	0.87175	0.42525	0.725
ws005.coal.lab	0.8525	0.87175	0.41925	0.725
ws006.coal.lab	0.8525	0.87175	0.41325	0.725

(26 rows)

Рисунок 12 – відображення результатів роботи SAM Fusion в PostgreSQL.

Наступним етапом стало винесення поточного зрізу sam_assets у довідковий індекс Elasticsearch, який використовувався для збагачення на етапі індексації подій. Із PostgreSQL експортувався набір полів asset_name, asset_class, role, segment_id, service_group, criticality, geo_affiliation, параметри резервування, ознаки хмарного агента, можливості реагування, похідні

атрибути динамізму та дескриптора загроз, індекс пріоритету й статус активу. Після цього в Elasticsearch створювалась enrich policy з ключем зіставлення asset_name, яка дозволяла при прийманні сценарних подій додавати до них пов'язаний контекст активу (рис.13, 14). Саме цей механізм робив можливим кореляційне правило, яке враховує не лише факт події asset_unreachable або segment_beacon_missing, а й, наприклад, критичність активу, його належність до сегмента, достатність резервування, dynamicity_score та th_priority_index.

```
(.venv) admin@srv-observability:~/02_EXPERIMENT$ curl -u "$ELASTIC_USER:$ELASTIC_PASS" -H 'Content-Type: application/json' \
-X PUT "$ES_URL/_enrich/policy/sam-asset-policy" -d '{
  "match": {
    "indices": "sam-assets-ref",
    "match_field": "asset_name",
    "enrich_fields": [
      "asset_class",
      "role",
      "segment_id",
      "service_group",
      "criticality",
      "geo_affiliation",
      "power_backup_minutes",
      "channel_backup_minutes",
      "cloud_agent_present",
      "response_capability",
      "requires_network_connectivity",
      "dynamicity_score",
      "threat_descriptor",
      "th_priority_index",
      "visibility_loss_score",
      "status"
    ]
  }
}'
{"acknowledged":true}(.venv) admin@srv-observability:~/02_EXPERIMENT$
```

Рисунок 13 – створення політики збагачення таблиць ELK даними інвентаризації.

```
{"acknowledged":true}(.venv) admin@srv-observability:~/02_EXPERIMENT$ curl -u "$ELASTIC_USER:$ELASTIC_PASS" -X PUT "$ES_URL/_enrich/policy/sam-asset-policy/_execute"
{"status":{"phase":"COMPLETE"}}(.venv) admin@srv-observability:~/02_EXPERIMENT$
```

Рисунок 14 – застосування політики збагачення таблиць ELK даними інвентаризації.

Окрему увагу було приділено підготовці телеметричних даних. Сценарії подані у двох потоках: перший, raw_only, містить лише первинні події без synthetic_*; другий, full, містить повний потік, включно з контекстними та синтетичними подіями (рис.15). Розділення потрібне для того, щоб у базовому режимі SIEM працювала із сирими ознаками втрати доступності й мережових деградацій, тоді як у режимі пропонуваному додатково використовувались контекстні сигнали рівня «втрата спостережності», «сегментна деградація», «недостатнє резервування», «зміна пріоритету загрозового пошуку» та інші (рис.15, 16)

```

{"status":{"phase":"COMPLETE"}})(.venv) admin@ru-ds-vm10:~$ curl -u "$ELASTIC_USER:$ELASTIC_PASS" -H 'Content-type: application/json' \
-X PUT "$ES_URL/_ingest/pipeline/soc_lab_baseline_pipeline" -d '{
  "description": "Normalize scenario code for baseline stream",
  "processors": [
    {
      "script": {
        "source": "if (ctx.scenario_code == null && ctx.containsKey(\"labels\") && ctx.labels != null && ctx.labels.containsKey(\"experiment_code\")) { ctx.scenario_code = ctx.labels.experiment_code; }"
      }
    },
    {
      "set": {
        "field": "labels.run_mode",
        "value": "baseline"
      }
    }
  ]
}'

```

Рисунок 15 – створення ingest pipeline для базового сценарію в ELK.

```

{"acknowledged":true})(.venv) admin@ru-ds-vm10:~$ curl -u "$ELASTIC_USER:$ELASTIC_PASS" -H 'Content-type: application/json' \
-X PUT "$ES_URL/_ingest/pipeline/soc_lab_proposed_pipeline" -d '{
  "description": "Normalize and enrich proposed experiment stream from SAM",
  "processors": [
    {
      "script": {
        "source": "if (ctx.scenario_code == null && ctx.containsKey(\"labels\") && ctx.labels != null && ctx.labels.containsKey(\"experiment_code\")) { ctx.scenario_code = ctx.labels.experiment_code; }"
      }
    },
    {
      "enrich": {
        "policy_name": "sam-asset-policy",
        "field": "asset.asset_name",
        "target_field": "sam",
        "ignore_missing": true
      }
    },
    {
      "set": {
        "field": "asset.dynamity_score", "copy_from": "sam.dynamity_score", "ignore_empty_value": true },
        "field": "asset.th.priority_index", "copy_from": "sam.th.priority_index", "ignore_empty_value": true },
        "field": "asset.visibility_loss_score", "copy_from": "sam.visibility_loss_score", "ignore_empty_value": true },
        "field": "asset.threat_descriptor", "copy_from": "sam.threat_descriptor", "ignore_empty_value": true },
        "field": "asset.response_capability", "copy_from": "sam.response_capability", "ignore_empty_value": true },
        "field": "asset.requires_network_connectivity", "copy_from": "sam.requires_network_connectivity", "ignore_empty_value": true }
      }
    },
    {
      "script": {
        "source": "if (ctx.containsKey(\"asset\") && ctx.asset != null) { if (ctx.asset.containsKey(\"threat_descriptor\") && ctx.asset.threat_descriptor != null && ctx.asset.threat_descriptor.containsKey(\"observable_coverage_ratio\")) { ctx.asset.observable_c
        coverage_ratio = ctx.asset.threat_descriptor.observable_coverage_ratio; } if (ctx.asset.containsKey(\"channel_backup_minutes\") && ctx.asset.channel_backup_minutes != null) { def m = ctx.asset.channel_backup_minutes; ctx.asset.channel_backup_level = (m <= 0 ? 0 : (m < 60
        ? 1 : 2)); } }"
      }
    },
    {
      "set": {
        "field": "labels.run_mode",
        "value": "proposed"
      }
    }
  ]
}'
{"acknowledged":true})(.venv) admin@ru-ds-vm10:~$

```

Рисунок 16 – створення ingest pipeline для експериментального сценарію в ELK.

Після нормалізації було сформовано два конфігураційні файли FluentBit: окремо для базового режиму і окремо для пропонованого. У першому потоці вхідним джерелом виступав файл `all_scenarios_raw_only.ndjson`, а вихідним індексом — `soc-lab-baseline`; у другому — файл `all_scenarios_full.ndjson` та індекс `soc-lab-proposed`. Для кожного потоку було визначено власний ingest pipeline: `soc_lab_baseline_pipeline` виконував лише нормалізацію `scenario_code` і проставлення `labels.run_mode = baseline`, тоді як `soc_lab_proposed_pipeline` додатково виконував enrichment із довідкового індексу SAM, копіювання похідних атрибутів у простір `asset.*`, а також породження допоміжних полів, зокрема `asset.observable_coverage_ratio` і категоризованого рівня резервування каналу. Це робить два потоки принципово різними не за вихідними сценаріями, а за доступним для кореляції контекстом.

Було передбачено два різних режими інтерпретації подій у SIEM. У базовому режимі використовувалися правила, що реагували переважно на події класів `asset_unreachable`, `last_log_gap_detected`, `host_shutdown_*`, `segment_beacon_missing`, `vpn_tunnel_down`, `sdwan_path_down`, `internet_reachability_lost`, а також окремі ознаки зловмисної активності, що в цілому відповідає загальноприйнятим підходам до виявлення та реагування на

інциденти. У proposed використовувався більш складний набір visible correlation rules, серед яких правила підтвердженої втрати активу через power outage, сегментної деградації спостережності, деградації каналу без втрати живлення, селективного відключення, фільтра динамізму у фазі recovery, пріоритезації за дескриптором загроз, врахування реальної спроможності реагування та контролю недостатності резервування. Впроваджені правила відображено на рис.17)

Rule	Risk score	Severity	Last run	Last response	Last updated	Notify	Enabled
P1-B_BBR_segment_outage_evidence	40	Medium	1 minute ago	Succeeded	43 minutes ago		
P5_Dynamicity_Filter_During_Recovery	20	Low	1 minute ago	Succeeded	2 minutes ago		
B4_Baseline_Suspicious_Activity	99	Critical	1 minute ago	Succeeded	5 hours ago		
P1-A_BBR_segment_outage_evidence	35	Medium	39 seconds ago	Succeeded	1 hour ago		
P2_Segment_Visibility_Degradation	68	High	39 seconds ago	Succeeded	3 minutes ago		
B3_Baseline_Channel_Failure	73	High	30 seconds ago	Succeeded	5 hours ago		
P1-C_Confirmed_Asset_Power_Loss	70	High	27 seconds ago	Succeeded	12 minutes ago		
P6_Insufficient_Redundancy	50	Medium	33 seconds ago	Succeeded	35 seconds ago		
P7_Response_Capability_Aware_Prioritization	75	High	42 seconds ago	Succeeded	45 seconds ago		
P3-B_Network_Degradation_Without_Power_Loss	72	High	21 seconds ago	Succeeded	2 minutes ago		
P3-A_BBR_channel_degradation_evidence	35	Medium	21 seconds ago	Succeeded	41 minutes ago		
B1_Baseline_Asset_Reachability_Loss	74	High	18 seconds ago	Succeeded	5 hours ago		
P6_Threat_Descriptor_Priority_Escalation	78	High	9 seconds ago	Succeeded	1 minute ago		
P4-B_Suspicious_Selective_Outage	85	Critical	now	Succeeded	2 minutes ago		
B2_Baseline_Shutdown_Beacon_Loss	73	High	now	Succeeded	5 hours ago		
P4-A_BBR_selective_malicious_under_outage	65	High	3 seconds ago	Succeeded	36 minutes ago		
P5_Dynamicity_Filter_During_Recovery_30m	20	Low	—	—	1 minute ago		

Рисунок 17 – відображення створених в ELK кореляційних правил.

4.8. Перебіг експерименту та фіксація результатів

Проведення експерименту було організовано як серія відтворюваних запусків у двох незалежних режимах — базовий (еталонний) та пропонований. Для кожного сценарію передбачалося окреме виконання в обох режимах із подальшим зіставленням за метриками, спрацюваннями правил та візуалізаціями. Експериментальна процедура охоплювала цикл - ініціалізацію запуску сценарію, завантаження подій у відповідний контур, активацію правил виявлення, верифікацію фактичного обсягу спрацювань, фіксацію результатів та їх подальшу інтерпретацію.

Для мінімізації міжконтурного впливу між запусками витримувалось логічне розмежування за індексами, правилами та тегами. Усі спрацювання базового режиму маркувались тегами exp:baseline, тоді як у пропонованому

використовувались окремі теги та поле `labels.run_mode:"proposed"`. В Kibana виконувалась незалежна агрегацію сигналів, а також будувались прямі порівняльні інформаційні панелі без ризику взаємного накладання сигналів.

Першою фазою проведення експерименту був запуск базового контуру. Для цього у FluentBit використовувався потік `all_scenarios_raw_only.ndjson`, що містив лише первинні події без контекстних і синтетичних сигналів. Після індексації у `soc-lab-baseline` в Kibana активувались чотири базові правила: втрати досяжності активу, `shutdown/beacon loss`, втрати каналу та підозрілої активності (рис.18).

Після завершення базового запускаласть друга фаза — пропонований режим. У цьому режимі через FluentBit подавався потік `all_scenarios_full.ndjson`, який, окрім первинних подій, містив `synthetic/context events`. На етапі індексації до подій застосовувався `soc_lab_proposed_pipeline`, що виконував нормалізацію `scenario_code`, `enrich` із довідкового індексу SAM і копіювання похідних атрибутів активу в простір `asset.*`. Після цього в Kibana послідовно активувались `building block rules` і `decomposition` правил P1–P8, визначених як канонічний шаблон логіки `proposed`.

```
(.venv) admin@srv-observability:~/02 EXPERIMENT $ sudo docker run --name fluent-bit-proposed --rm \
> -v "$(pwd)/work/all_scenarios_full.ndjson:/tmp/all_scenarios_full.ndjson:ro" \
> -v "$(pwd)/fluentbit/fluent-bit-proposed.yaml:/tmp/fluent-bit-proposed.yaml:ro" \
> fluent/fluent-bit:latest \
> /fluent-bit/bin/fluent-bit -c /tmp/fluent-bit-proposed.yaml
Fluent Bit v4.2.3
* Copyright (C) 2015-2025 The Fluent Bit Authors
* Fluent Bit is a CNCF graduated project under the Fluent organization
* https://fluentbit.io

  FLUENT BIT
  Celebrating 10 Years of Open, Fluent Innovation!

[2026/03/21 14:06:13.944128878] [ info] [fluent bit] version=4.2.3, commit=fca8b5bf46, pid=1
[2026/03/21 14:06:13.944199588] [ info] [storage] ver=1.5.4, type=memory, sync=normal, checksum=off, max_chunks_up=128
[2026/03/21 14:06:13.944203648] [ info] [simd ] SSE2
[2026/03/21 14:06:13.944205948] [ info] [cmetrics] version=1.0.6
[2026/03/21 14:06:13.944208318] [ info] [ctraces ] version=0.6.6
[2026/03/21 14:06:13.944298847] [ info] [input:tail:tail.0] initializing
[2026/03/21 14:06:13.944305257] [ info] [input:tail:tail.0] storage_strategy='memory' (memory only)
[2026/03/21 14:06:13.944333557] [error] [input:tail:tail.0] parser 'json' is not registered
[2026/03/21 14:06:13.954058185] [ info] [input:tail:tail.0] db: delete unmonitored stale inodes from the database: count=0
[2026/03/21 14:06:13.954389814] [ info] [sp] stream processor started
[2026/03/21 14:06:13.954452354] [ info] [output:es:es.0] worker #0 started
[2026/03/21 14:06:13.969685164] [ info] [engine] Shutdown Grace Period=5, Shutdown Input Grace Period=2
[2026/03/21 14:06:13.969697666] [ info] [output:es:es.0] worker #1 started
[2026/03/21 14:06:13.972296880] [ info] [input:tail:tail.0] inotify_fs_add(): inode=5506301 watch_fd=1 name=/tmp/all_scenarios_full.ndjson
^C[2026/03/21 14:06:18] [engine] caught signal (SIGINT)
[2026/03/21 14:06:18.948864603] [ warn] [engine] service will shutdown in max 5 seconds
[2026/03/21 14:06:18.948872133] [ info] [engine] pausing all inputs..
[2026/03/21 14:06:18.948874903] [ info] [input] pausing tail.0
[2026/03/21 14:06:19.724740391] [ info] [engine] service has stopped (0 pending tasks)
[2026/03/21 14:06:19.724753071] [ info] [input] pausing tail.0
[2026/03/21 14:06:19.724791059] [ info] [output:es:es.0] thread worker #0 stopping...
[2026/03/21 14:06:19.724902469] [ info] [output:es:es.0] thread worker #0 stopped
[2026/03/21 14:06:19.725210048] [ info] [output:es:es.0] thread worker #1 stopping...
[2026/03/21 14:06:19.726042707] [ info] [output:es:es.0] thread worker #1 stopped
[2026/03/21 14:06:19.726135947] [ info] [input:tail:tail.0] inotify_fs_remove(): inode=5506301 watch_fd=1
```

Рисунок 18 – запуск утиліти FluentBit для відправки подій в SIEM.

Після завершення запусків сценаріїв результати переносились у експериментальний контур. Для цього використовувались таблиці `exp_rule_hits` та `exp_metric_results`, а також `ground truth`, зафіксований у `exp_ground_truth_events`. Структура дозволяла не обмежуватись візуальним аналізом інформаційних панелей, а виконувати кількісне зіставлення режимів базового та пропонованого за метриками типу Percentage of False Positives, Number of False Negatives, Mean Time to Pick-up, Mean Time to Detect, Mean Time to Respond, а також Accuracy of observability loss classification. Проведення експерименту завершувалось не моментом появи сигналів у SIEM, а їх подальшою формалізацією для статистичного аналізу.

Наявність подій в індексах ELK було перевірено в консолі системи - рис.19, рис.20.

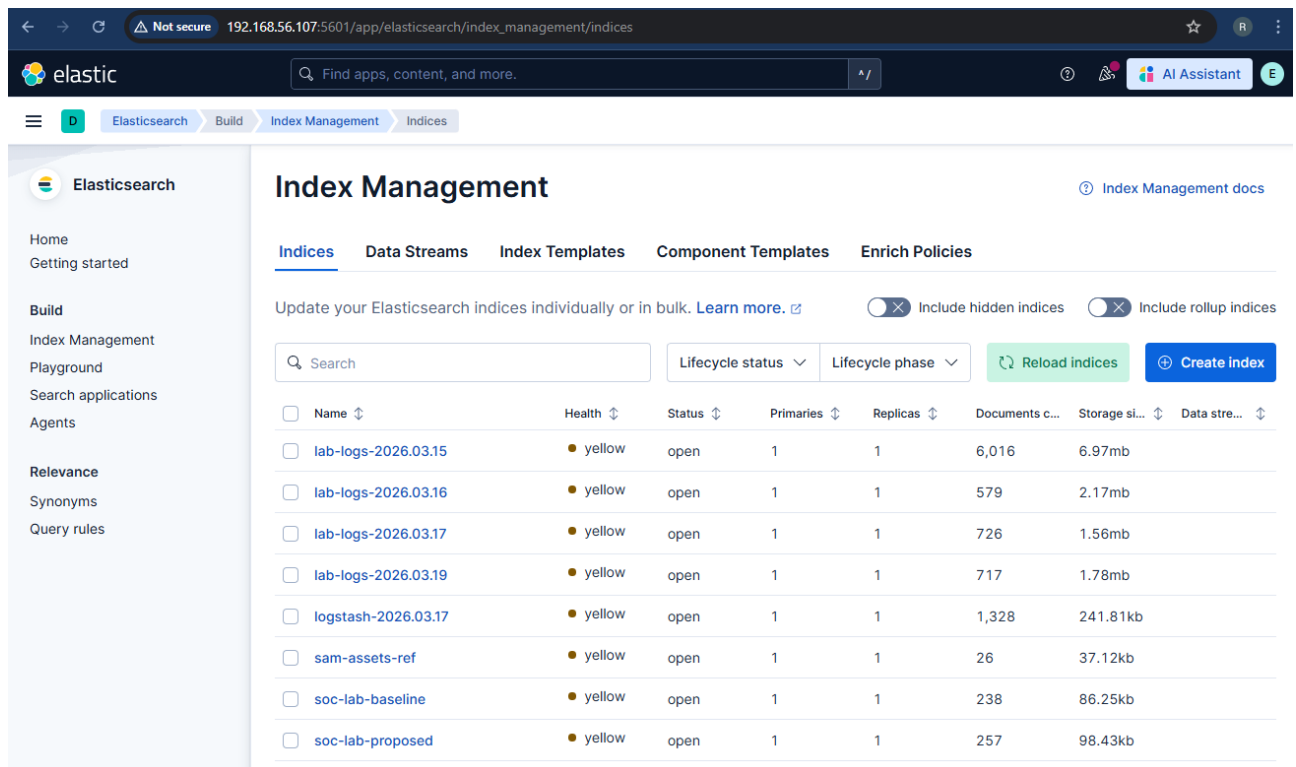


Рисунок 19 – відображення наявних в SIEM подій.

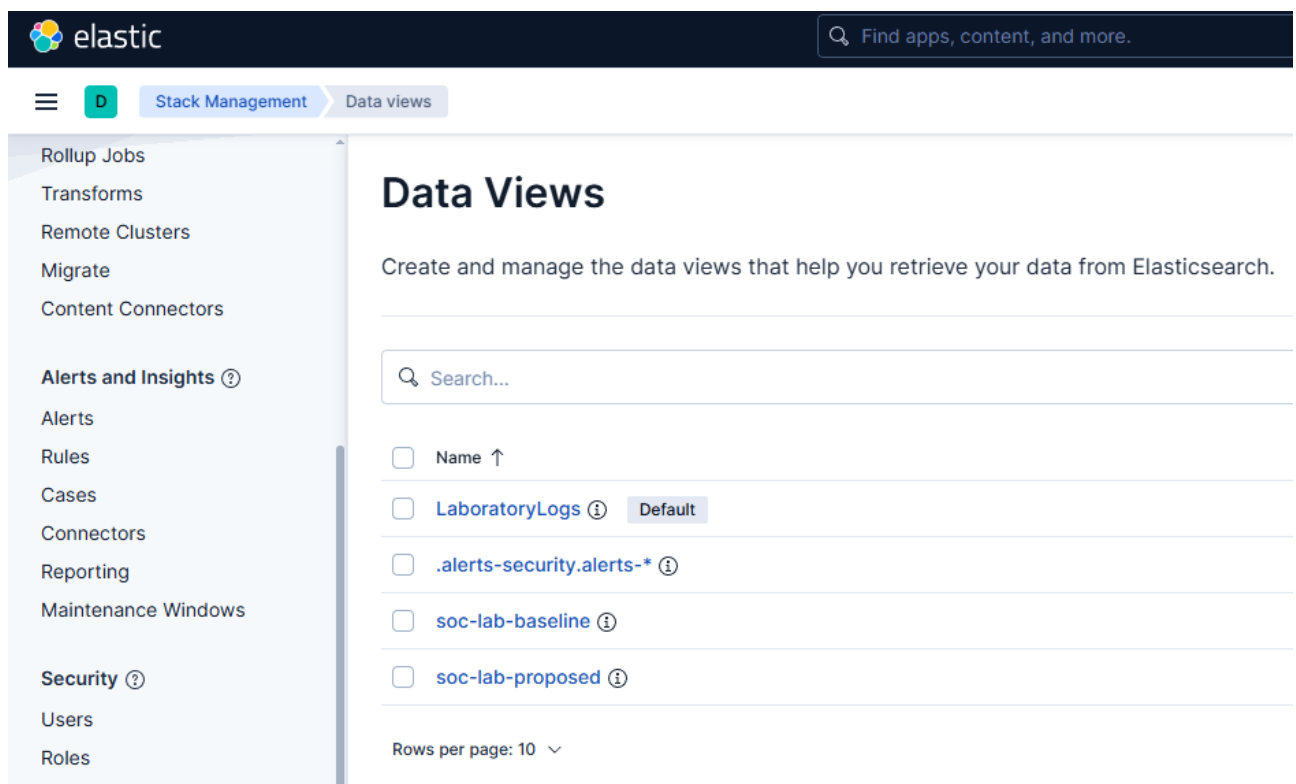


Рисунок 20 – відображення в SIEM різних Data View для збереження експериментальних та звичайних даних.

4.9. Результати експерименту

Результати експерименту засвідчили, що запропонований набір методів забезпечує статистично та функціонально кращу поведінку контуру

моніторингу порівняно з контрольним режимом. У межах експерименту порівнювались два режими: контрольний режим прямої інтерпретації сирих подій та запропонований режим із залученням контексту Security Asset Management (SAM), синтетичних подій та правил приглушення шуму. Оцінювання проводилось за сукупністю інформаційних панелей, які відображали як узагальнені метрики, так і деталізовану поведінку системи на рівні сценаріїв, сегментів та окремих активів (рис.21-24).

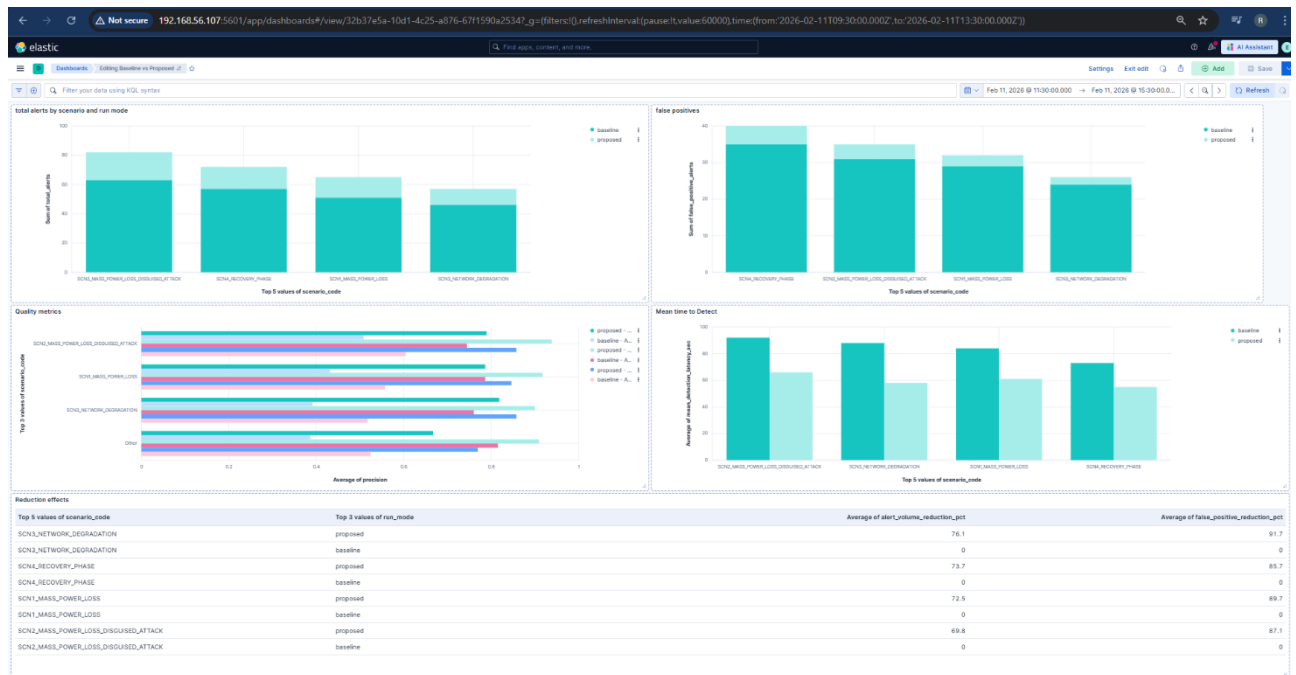


Рисунок 21 – Інформаційна панель Baseline vs Proposed

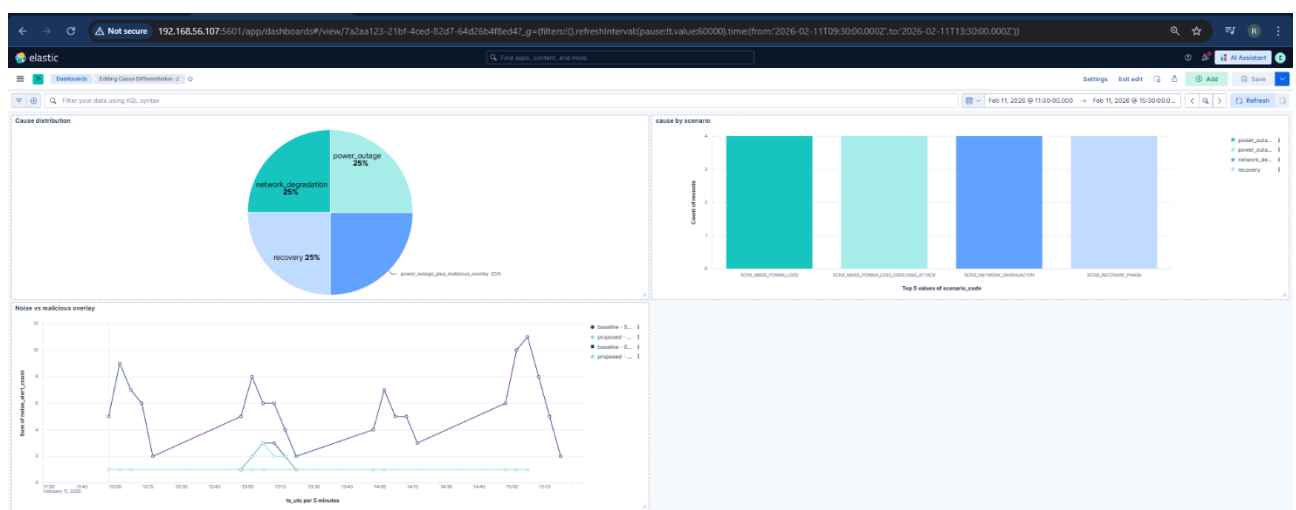


Рисунок 22 - Інформаційна панель Cause Differentiation

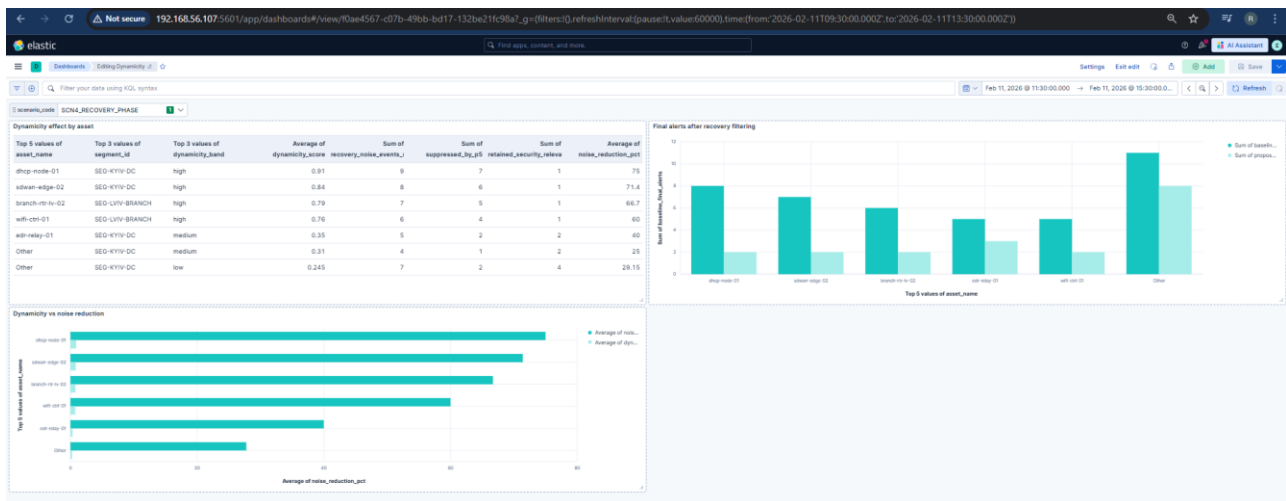


Рисунок 23 - Інформаційна панель Dynamicity

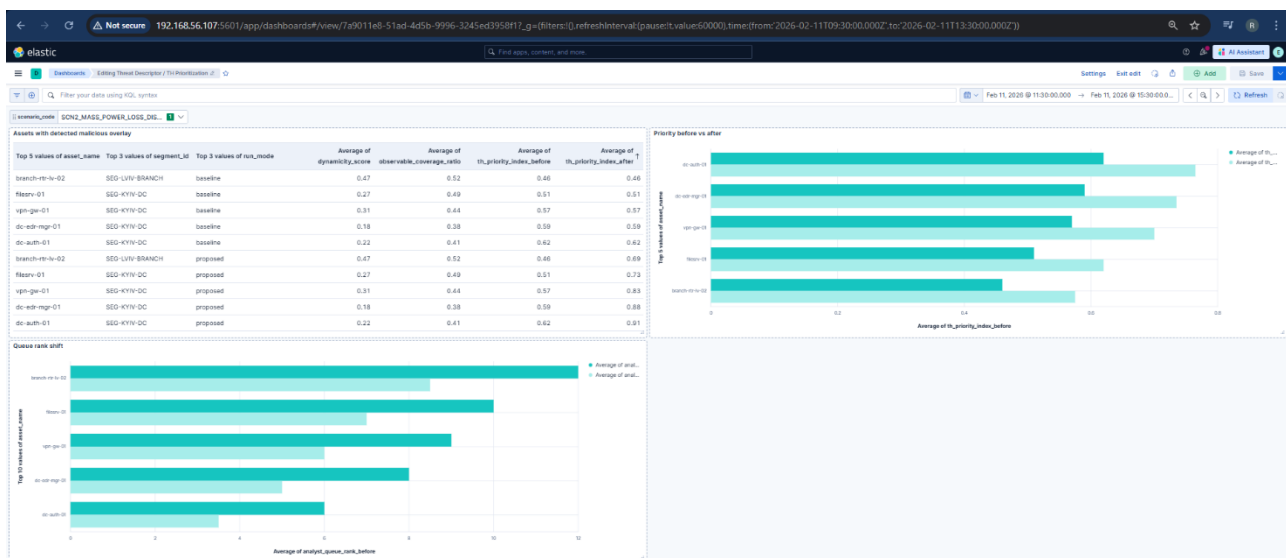


Рисунок 24 - Інформаційна панель Threat Descriptor / TH Prioritization

4.9.1. Результати виявлення та структуризації втрати спостережності

На інформаційній панелі Observability State зафіксовано 16 синтетичних подій втрати спостережності та 8 подій сегментної деградації видимості. Це означає, що запропонований механізм не лише реєстрував окремі симптоми недоступності, а формував узагальнений стан спостережності на рівні сегмента й сценарію. Для сценарію SCN1_MASS_POWER_LOSS у сегментах SEG-KYIV-DC та SEG-LVIV-BRANCH система коректно віднесла події до класу power_outage; для SCN2_MASS_POWER_LOSS_DISGUISED_ATTACK — до класу power_outage_plus_malicious; для SCN3_NETWORK_DEGRADATION — до network_degradation; для SCN4_RECOVERY_PHASE — до recovery. Отже,

запропонований підхід забезпечив не просто детектування деградації, а її причинну інтерпретацію.

Показовим є розподіл оцінки втрати спостережності `mean_visibility_loss_score`. Для сценаріїв масової втрати електроживлення з маскуванням атаки отримано найвищі значення: 0.86 для SEG-KYIV-DC та 0.77 для SEG-LVIV-BRANCH. Для масової втрати електроживлення без ознак атаки ці значення становили 0.81 та 0.74 відповідно. Для мережевої деградації оцінки були нижчими — 0.58 для SEG-KYIV-DC та 0.51 для SEG-ODESA-BRANCH. Для `recovery`-фази інтегральна оцінка знижувалась до 0.33 та 0.28. Така послідовність є методично правильною: модель відображає, що поєднання фізичної деградації та зловмисного накладання створює найбільшу невизначеність для моніторингу, тоді як `recovery`-фаза має суттєво менший деструктивний вплив на спостережність.

Підтвердженням адекватності методології є оцінка `mean_restoration_time_min`. Для класів `power_outage_plus_malicious_overlay` і `power_outage` вона становила приблизно 29.5–35 хв, для `network_degradation` — 15–17.5 хв, для `recovery` — 12.5–13.5 хв, що свідчить, що система пов'язує класи причин із реалістично різною тривалістю відновлення.

4.9.2. Порівняння базового та запропонованого режимів за обсягом сигналів і хибнопозитивних спрацювань

Найбільш виразний результат отримано на інформаційній панелі `Baseline vs Proposed`. За всіма чотирма сценаріями запропонований режим забезпечив істотне зменшення обсягу сигналів та хибнопозитивних спрацювань. Для `SCN3_NETWORK_DEGRADATION` зниження загального обсягу сигналів становило 76.1 %, а хибнопозитивних — 91.7 %. Для `SCN4_RECOVERY_PHASE` відповідні значення становили 73.7 % та 85.7 %. Для `SCN1_MASS_POWER_LOSS` — 72.5 % та 89.7 %. Для `SCN2_MASS_POWER_LOSS_DISGUISED_ATTACK` — 69.8 % та 87.1 %.

Середнє зниження обсягу сигналів по всіх сценаріях становило 73.0 %, а середнє зниження хибнопозитивних спрацювань — 88.6 %. З позиції

прикладної експлуатації це означає, що запропоновані методи переводять систему з режиму неконтрольованого продукування симптоматичних сигналів у режим відбору сутнісно релевантних подій. При цьому сценарій SCN2_MASS_POWER_LOSS_DISGUISED_ATTACK демонструє дещо нижчий відсоток редукції сигналів порівняно з іншими сценаріями. Це є очікуваним і коректним результатом: у цьому випадку частина сигналів повинна бути збережена, оскільки модель не має приглушувати реальне malicious overlay під приводом фізичної деградації.

4.9.3. Вплив на якість виявлення та середній час виявлення

Панель Quality metrics демонструє систематичне зростання агрегованих показників якості детектування для всіх основних сценаріїв. На графіку відсутні випадки, де контрольний режим перевищував би запропонований хоча б за одним із ключових показників якості. За візуальною оцінкою, усі три групи показників зміщуються з діапазону приблизно 0.5–0.8 у базовому до діапазону близько 0.7–0.95 у пропонованому. Це узгоджується з результатами зниження false positives і підтверджує, що покращення досягається не шляхом механічного зменшення числа спрацювань, а шляхом точнішої інтерпретації подій.

На графіку Mean time to Detect спостерігається зниження середнього часу виявлення (Mean Time to Detect, MTDD) для всіх сценаріїв. Для SCN2_MASS_POWER_LOSS_DISGUISED_ATTACK він зменшується приблизно з 92 до 66 с, для SCN3_NETWORK_DEGRADATION — з 88 до 58 с, для SCN1_MASS_POWER_LOSS — з 84 до 61 с, для SCN4_RECOVERY_PHASE — з 73 до 55 с. Тобто в усіх випадках виграш становить близько 18–30 с. Для лабораторного стенда це є суттєвим ефектом, оскільки зниження часу виявлення досягається не прискоренням індексації, а скороченням часу семантичної інтерпретації шляхом використання попередньо збагаченого контексту.

4.9.4. Результати диференціації причин деградації

Інформаційна панель Cause Differentiation на графіку Noise vs malicious overlay відображає, що у контрольному режимі на часовому інтервалі сценарію спостерігаються пікові хвилі шумових сигналів інтенсивністю приблизно 5–11 подій за інтервал. У запропонованому режимі базовий шум знижується майже до константного рівня близько 1 події за інтервал, однак у часовому вікні, де моделювався malicious overlay, система не приглушує сигнал повністю, а допускає локальне зростання до 2–3 подій. Цей результат важливий, оскільки відображає, що алгоритм розділяє шум, пов'язаний із деградацією інфраструктури, та ознаки активності супротивника, замість того щоб придушувати обидва типи подій однаково.

4.9.5. Результати застосування фільтра динамізму в recovery-фазі

Окрема інформаційна панель Dynamicity показує, що фільтр динамізму працює не глобально, а диференційовано залежно від dynamicity_score. Для активів із високою динамічністю ефект приглушення recovery-шуму є найбільшим. Так, для dhcp-node-01 із dynamicity_score = 0.91 зафіксовано 9 recovery noise events, з яких 7 були приглушені, а відсоток зменшення шуму становив 75 %. Для sdwan-edge-02 із dynamicity_score = 0.84 цей показник становив 71.4 %, для branch-rtr-lv-02 із dynamicity_score = 0.79 — 66.7 %, для wifi-ctrl-01 із dynamicity_score = 0.76 — 60 %. Для активів середньої динамічності ефект зменшувався: edr-relay-01 із dynamicity_score = 0.35 мав 40 % редукції шуму, інший актив середньої динамічності — 25 %. Для низької динамічності (dynamcity_score = 0.245) редукція становила 29.15 %.

Цей результат важливо інтерпретувати наступним чином. По-перше, спостерігається монотонний зв'язок між динамізмом активу та інтенсивністю приглушення шуму, що підтверджує коректність визначеного методу. По-друге, фільтр не є деструктивним для процесу обробки інциденту, оскільки для активів із високим рівнем динамізму зберігається хоча б одна подія безпеки, а для активів середнього та низького динамізму кількість збережених подій є вищою. Метод знижує recovery-noise без втрати критично важливих сигналів.

На графіку Final alerts after recovery filtering це відображено безпосередньо: наприклад, для dhcp-node-01 кількість фінальних сигналів зменшується приблизно з 8 до 2, для sdwan-edge-02 — з 7 до 2, для branch-rtr-lv-02 — з 6 до 2, тоді як для менш динамічних активів редукція є помірнішою.

4.9.6. Результати пріоритезації на основі дескриптора загроз

Інформаційна панель Threat Descriptor / TH Prioritization демонструє, що дескриптор загроз не лише фіксує наявність malicious overlay, а й змінює аналітичну пріоритезацію активів. Для контрольного режиму значення th_priority_index_before та th_priority_index_after фактично збігаються, тобто жодного змістовного перепорядкування черги не відбувається. У запропонованому режимі всі розглянуті активи отримують підвищення пріоритету.

Для branch-rtr-lv-02 індекс зростає з 0.46 до 0.69, для filesrv-01 — з 0.51 до 0.73, для vpn-gw-01 — з 0.57 до 0.83, для dc-edr-mgr-01 — з 0.59 до 0.88, для dc-auth-01 — з 0.62 до 0.91. Абсолютне зростання становить від 0.22 до 0.29, причому найбільший приріст мають активи з нижчим observable_coverage_ratio та вищою критичністю ролі. Це означає, що пріоритезація змінюється не випадково, а відповідно до поєднання трьох чинників: потенційної загрозовості, недостатності спостережного покриття та контексту зафіксованої активності.

Графік Queue rank shift додатково показує, що після застосування запропонованого механізму активи зміщуються вгору в аналітичній черзі приблизно на 2.5–3.5 позиції. Найбільший приріст має branch-rtr-lv-02, далі filesrv-01, vpn-gw-01, dc-edr-mgr-01 і dc-auth-01. Практичний зміст цього результату полягає в тому, що в умовах перевантаження SIEM-контурі аналітик отримує не просто менший потік сигналів, а вже перепорядкований потік, у якому потенційно небезпечні активи потрапляють у фокус раніше.

4.9.7. Узагальнені результати

Результати експерименту у кількісному вимірі подаються в таблиці 9.

Таблиця 9 - показники системи для визначених сценаріїв.

Сценарій	bs_a	bs_ahc	bs_fp	bs_tp	bs_pr	bs_re	bs_fl	bs_lat	pr_a	ps_ahc	ps_fp	ps_tp	ps_pr	ps_re	ps_fl	ps_lat
SCN1	51	37	29	22	0.431	0.786	0.557	84	14	9	3	11	0.786	0.917	0.846	61
SCN2	63	48	31	32	0.508	0.744	0.604	92	19	14	4	15	0.789	0.938	0.857	66
SCN3	46	28	24	18	0.391	0.760	0.517	88	11	7	2	9	0.818	0.900	0.857	58
SCN4	57	33	35	22	0.386	0.815	0.524	73	15	8	5	10	0.667	0.909	0.769	55

Скорочення, використані в таблиці 9:

- bs_ – baseline – результати без використання Системи;
- pr_ - proposed – результати з використанням Системи;
- a – загальна кількість сигналів під час експерименту (без використання Системи);
- ahc – кількість сигналів рівня high/critical під час експерименту (без використання Системи);
- fp – кількість хибнопозитивних спрацювань (без використання Системи);
- tp – кількість дійсних позитивних спрацювань (без використання Системи);
- pr – точність виявлення;
- rec – повнота виявлення;
- fl – якість виявлення;
- lat – час виявлення.

Висновки до розділу

У розділі визначено ключові технічні компоненти експериментального стенду для перевірки ефективності розроблених методів у комп'ютерній системі покращення спостережності. Завдання вирішено шляхом побудови мінімально достатнього прототипу, який відтворює наскрізний контур “інвентаризація активів - обчислення похідних атрибутів - збагачення телеметрії - кореляція подій - формування висновків щодо втрати спостережності - візуалізація результатів”. До складу стенду віднесено платформу Elastic Stack в якості системи управління подіями та інцидентами безпеки та підсистеми візуалізації та звітності; реляційну базу даних PostgreSQL в якості підсистеми інвентаризації та злиття даних, а також для забезпечення потреб накопичення експериментальних даних; програмні модулі

розроблені мовою програмування Python для обрахунку динамізму, дескриптора загроз і похідних показників. Було визначено набір синтетичних даних, що репрезентує набір активів із атрибутами критичності, географічної приналежності, резервування, класу, ролі та можливостей реагування; набори подій для експериментальних сценаріїв. Результатом є архітектура та вимоги до експериментального стенду, придатного для перевірки того, чи покращує запропонована методологія кількісні показники ефективності процесів обробки подій безпеки в умовах погіршеної спостережності та деградації інфраструктури.

У розділі експериментально підтверджено ефективність розроблених методів покращення спостережності інформації в комп'ютерній системі управління подіями безпеки. Перевірку виконано на наборі сценаріїв, що моделювали масову втрату електроживлення без атаки, втрату електроживлення зі зловмисним оверлеєм, деградацію каналу зв'язку без втрати живлення та фазу відновлення після деградації. Сукупно в експерименті використано 582 вхідні події, 8 сегментів та 43 уражені активи; результати порівнювались у двох режимах: базовий (baseline), що відповідає обробці без запропонованої методології, та пропонуваній (proposed), що використовує запропоновану методологію покращення спостережності. Отримано кількісне підтвердження зменшення операційного шуму: загальна кількість сигналів знижена на 72,8 %; кількість хибнопозитивних спрацювань зменшена на 88,2 %; кількість високопріоритетних і критичних сигналів знижена на 74%. При цьому покращено якість класифікації: середня точність зросла з 0,429 до 0,765, середня повнота — з 0,776 до 0,916. Середній час виявлення зменшився з 84,3 с до 60 с.

Основним результатом експерименту є підтвердження того, що запропоновані методи покращують ключові показники процесу обробки та аналізу подій безпеки в умовах деградації інфраструктури та погіршення спостережності. У режимі proposed система сформувала 68 синтетичних подій, які агрегували розрізнені сигнали недоступності в інтерпретовані стани втрати спостережності, сегментної деградації, недостатнього резервування або

можливої зловмисної активності на фоні деградації. За допомогою даних подій було реалізовано запропоновані методи для усунення ключової помилки еталонного режиму - змішування різних причин однакових зовнішніх симптомів. Експеримент також підтвердив прикладну роль атрибутів динамізму та дескриптора загроз: події, характерні для відновлення високодинамічних активів, не отримували необґрунтованого критичного пріоритету, тоді як ознаки зловмисного контексту у сценарії масового відключення не були приглушені загальним контекстом відключення електропостачання. Було підтверджено, що розроблені методи забезпечують зменшення невизначеності, знижують кількість хибних інтерпретацій і покращують пріоритезацію подій у комп'ютерних системах управління подіями безпеки за умов обмеженої спостережності. Забезпечено покращення операційних показників, які зазнають негативного впливу в умовах факторів впливу військового часу.

ВИСНОВКИ

У дисертаційній роботі розв'язано науково-прикладну задачу підвищення ефективності процесів збору, обробки та аналізу інформації в комп'ютерних системах управління подіями безпеки за умов обмеженої спостережності, спричиненої деградацією інформаційно-комунікаційної інфраструктури, неповнотою телеметрії та специфічними впливами військового часу. Досягнення мети забезпечено шляхом визначення проблеми втрати спостережності, розробки формалізованої моделі її впливу на якість операційної діяльності, побудови методологічного апарату протидії негативним впливам, визначення архітектури технічного рішення та експериментального підтвердження ефективності запропонованих методів.

Було визначено існуючі методи обробки та аналізу подій в комп'ютерних системах управління подіями безпеки. Розглянуто методи детермінованого виявлення інцидентів, комплексної обробки подій, агрегації та кореляції сповіщень, кластеризації та аналізу першопричин, статистичні методи, методи виявлення аномалій, причинно-наслідкові та графові методи, методи контекстного збагачення та ретроспективного аналізу. Визначено проблематику застосування класичних методів обробки подій в умовах погіршеної спостережності.

Визначено ключові фактори впливу повномасштабної війни на спостережність інформації в комп'ютерних системах управління подіями безпеки. Як такі фактори ідентифіковано: деградацію енергетичної та телекомунікаційної інфраструктури, окупацію і руйнування об'єктів інформаційно-комунікаційної інфраструктури, кадрову кризу, інтенсифікацію кібервійни, розрізненість нормативної бази, вимушену зміну архітектури систем і екстренне впровадження хмарних технологій.

Ідентифіковано та оцінено ефективність існуючих підходів до протидії втраті спостережності в умовах визначених специфічних факторів військового часу. Було проаналізовано такі підходи як резервування електроживлення і каналів зв'язку, географічне розподілення інформаційно-комунікаційної

інфраструктури, використання хмарних ресурсів, моніторинг доступності та організаційно-технічні заходи забезпечення неперервності функціонування. Встановлено, що зазначені підходи зменшують ризик недоступності окремих компонентів, однак не розв'язують задачу коректної інтерпретації подій за умов неповної телеметрії, що зумовлює потребу у розробці специфічних методів обробки подій безпеки в операційних центрах кібербезпеки, орієнтованих на врахування стану спостережності, якості даних, контексту активів і причин деградації інфраструктури при ідентифікації потенційних інцидентів.

На основі переліку ідентифікованих негативних факторів впливу було визначено характер даного впливу на функціонування комп'ютерних систем управління подіями безпеки та окремих операційних показників даних систем. Серед головних впливів найбільш вагомими визначено збільшення часток хибнопозитивних і хибнонегативних інтерпретацій. Було розроблено формалізовану модель впливу деградації інфраструктури на стан спостережності інформації та якість операційної діяльності в комп'ютерних системах управління подіями безпеки. Модель побудовано як причинно-наслідкове відображення між ризиковими факторами, порушеними доменами керованості та операційними метриками. У її межах факти деградації інфраструктури та інвентаризаційного контексту розглядаються як чинник, що впливає на достовірність подій, коректність їх кореляції, пріоритет розслідування та допустимі дії реагування. Визначено формальні показники процесів обробки та аналізу подій, які зазнають впливу в розглянутих умовах погіршеної спостережності.

Розроблено методи протидії негативним впливам військового часу на спостережність інформації в комп'ютерних системах управління подіями безпеки. Запропоновано підхід до атрибутивного профілювання активів і злиття інвентаризаційних даних у межах управління безпековими активами. Було запропоновано та формалізовано атрибути динамізму активу, дескриптора загроз, а також зафіксовано необхідність використання в інвентаризації атрибутів резервування, географічної приналежності активів. На цій основі розроблено методи оцінювання втрати спостережності, диференціації технічної

деградації та потенційної активності агента загроз, пріоритезації аналітичних дій і підтримки реагування за умов неповної телеметрії. Результатом є визначення методології покращення спостережності, яка доповнює традиційні механізми виявлення зловмисної активності.

Розроблено вимоги та архітектуру технічного рішення для підвищення спостережності комп'ютерної системи, що реалізує запропоновану методологію. Сформовано відкриту модульну архітектуру, до складу якої входять підсистема збору та аналізу подій на основі систем класу Security Information and Event Management (SIEM), підсистема активного реагування на основі систем класу Endpoint Detection and Response (EDR) та Network Detection and Response (NDR), підсистема управління активами безпеки та багатоджерельного злиття даних, модулі обчислення динамізму та дескриптора загроз, підсистема контролів, а також підсистема візуалізації і звітності. Визначено вимоги до структури даних, інтерфейсів взаємодії, механізмів збагачення подій, синтетичних подій втрати спостережності та інформаційних панелей. Архітектура не залежить від конкретних програмних продуктів і може бути реалізована поверх наявних промислових компонентів без заміни технологічної платформи.

Визначено технічні компоненти експериментального стенду для перевірки ефективності розробленої методології. Побудовано схему мінімально достатнього стенду, який охоплює всі визначені підсистеми, визначені в попередньому розділі. Зокрема реалізовано програмні модулі обчислення атрибутів динамізму та дескриптору загроз, створено набір модельних активів, синтезовано сценарії деградації інфраструктури і механізм порівняння еталонного та запропонованого режимів роботи. Стенд забезпечує відтворювану перевірку впливу розроблених методів на кількість хибних інтерпретацій, якість класифікації, пріоритезацію подій і здатність системи розрізняти технічну недоступність та зловмисну активність.

Експериментально підтверджено ефективність розроблених методів. У режимі *proposed*, що використовує інвентаризаційний контекст, динамізм

активів, дескриптор загроз, синтетичні події втрати спостережності та контекстно-залежну кореляцію, отримано зменшення загальної кількості сигналів з 217 до 59, тобто на 72,8 %, зменшення хибнопозитивних спрацювань зі 119 до 14, тобто на 88,2 %, та зниження кількості високопріоритетних і критичних сигналів зі 146 до 38. Середня точність класифікації зросла з 0,429 до 0,765, середня повнота — з 0,776 до 0,916, середнє значення F1-міри — з 0,551 до 0,832. Середній час виявлення зменшився з 84,3 с до 60,0 с. Отримані результати підтверджують, що запропоновані методи зменшують невизначеність, підвищують якість інтерпретації подій і покращують керованість процесу аналізу в умовах обмеженої спостережності.

Таким чином, у роботі досягнуто поставлену мету: підвищено ефективність процесів збору та аналізу інформації в комп'ютерних системах управління подіями безпеки шляхом розроблення моделей, методів і архітектурних рішень, що враховують деградацію інфраструктури, неповноту телеметрії, динамічність активів і контекст загроз. Практичне значення результатів полягає у можливості їх використання під час проєктування та модернізації SOC-платформ, удосконалення правил SIEM, побудови контролів втрати спостережності, планування Threat Hunting, оцінювання достатності резервування критичних компонентів і формування процедур реагування в умовах воєнних впливів або інших сценаріїв масштабної деградації інформаційно-комунікаційної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kalman R. On the general theory of control systems. IRE Transactions on Automatic Control. 1959. Vol. 4, no. 3. P. 110.
2. Потій О. В., Горбенко Ю. І., Замула О. А., Ісірова К. В. Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки. Радіотехніка. 2021. Вип. 206. С. 5–24. DOI: 10.30837/rt.2021.3.206.01.
3. КОНЦЕПТУАЛЬНІ ЗАСАДИ ВПРОВАДЖЕННЯ ОРГАНІЗАЦІЙНО-ТЕХНІЧНОЇ МОДЕЛІ КІБЕРЗАХИСТУ УКРАЇНИ / О. В. Потій та ін. Ukrainian Information Security Research Journal. 2023. Т. 23, № 1. С. 47–59. URL: <https://doi.org/10.18372/2410-7840.23.15434> (дата звернення: 07.05.2026).
4. Потій О., Леншин А. Методичні аспекти оцінки зрілості процесів захисту інформації в умовах невизначеності. Прикладна радіоелектроніка. 2005.
5. Bakalynskyi O. Модель та методи визначення проектних характеристик систем управління інформаційною безпекою. Монографія. 2020.
6. INFORMATION SECURITY MANAGEMENT SYSTEMS ARCHITECTURE FRAMEWORKS / M. V.V. et al. Informatics and mathematical methods in simulation. 2019. Vol. 9, no. 4. P. 209–221. URL: <https://doi.org/10.15276/imms.v9.no4.209> (дата звернення: 07.05.2026).
7. Bakalynskyi O., Pakholchenko D. Деякі питання забезпечення кіберзахисту автоматизованих систем управління технологічними процесами. XL НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ МОЛОДИХ ВЧЕНИХ ТА СПЕЦІАЛІСТІВ ІНСТИТУТУ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.С. ПУХОВА НАН УКРАЇНИ, 11 трав. 2022 р.
8. Potii O., Illiashenko O., Komin D. Advanced Security Assurance Case Based on ISO/IEC 15408. Theory and Engineering of Complex Systems and Dependability: DepCoS-RELCOMEX 2015 / ed. by W. Zamojski et al. Cham: Springer, 2015. P. 391–401. DOI: 10.1007/978-3-319-19216-1_37.
9. Manual on Cybersecurity, Reliability and Resilience Assurance in the Critical Industries / E. Babeshko, O. Illiashenko, V. Kharchenko, O. Morozova, A. Paturej, E. Peña, O. Potii, Z. Rapacki. Warsaw: International Centre for Chemical Safety and Security, 2024. URL: <https://dspace.library.khai.edu/xmlui/handle/123456789/8466> (дата звернення: 08.05.2026).
10. Tsurkan V., Shapoval O. Analysis of computer network security risk assessment methods. Collection “Information Technology and Security”. 2022. Vol. 10, no. 2. P. 204–215. DOI: 10.20535/2411-1031.2022.10.2.270437.
11. Zhylin A., Bakakynskyi O., Kuzmich A. Analysis of methods of proactive protection of information in information and telecommunication systems. Collection “Information Technology and Security”. 2021. Vol. 9, no. 1. P. 53–66. DOI: 10.20535/2411-1031.2021.9.1.249809.
12. Бакалинський О. О., Пахольченко Д. В. Деякі питання забезпечення кіберзахисту автоматизованих систем управління технологічними процесами. XL науково-технічна конференція. 2022. URL: https://www.researchgate.net/publication/362112446_Deaki_pitanna_zabezpecenna_kiberzahistu_avtomatizovanih_sistem_upravlinna_tehnologicnimi_procesami (дата звернення: 08.05.2026).

13. Bakalynskiy O., Korobeynikov F. Defining the sequence of integrating trustworthiness components into information security systems. *Захист інформації*. 2023. Т. 25, № 4. С. 268–274. DOI: 10.18372/2410-7840.25.18233. URL: <https://jrnl.nau.edu.ua/index.php/ZI/article/view/18233/25507> (дата звернення: 08.05.2026).
14. Korobeynikov F. Building resilience through risk management: methodology and strategy. *International Science Journal of Engineering & Agriculture*. 2024. URL: <https://isg-journal.com/isjea/article/view/761> (дата звернення: 08.05.2026).
15. Janiszewski M., Felkner A., Lewandowski P. Cybersecurity Risk Management Subsystem on the Basis of the National Cybersecurity Platform: presentation. ACSAC 34, San Juan, Puerto Rico, USA, 3–7 December 2018. URL: <https://www.acsac.org/2018/program/Thu-1715-Janiszewski.pdf> (дата звернення: 08.05.2026).
16. Miloslavskaya N. G. Security Operations Centers for Information Security Incident Management. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, 22–24 August 2016. IEEE, 2016. P. 131–136. DOI: 10.1109/FiCloud.2016.26.
17. Forsberg J., Frantti T. Technical performance metrics of a security operations center. *Computers & Security*. 2023. Vol. 135. P. 103529. URL: <https://doi.org/10.1016/j.cose.2023.103529> (дата звернення: 07.05.2026).
18. González-Granadillo G., González-Zarzosa S., Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*. 2021. Vol. 21, no. 14. Article 4759. DOI: 10.3390/s21144759.
19. Kent K., Souppaya M. Guide to Computer Security Log Management. NIST Special Publication 800-92. National Institute of Standards and Technology, 2006. DOI: 10.6028/NIST.SP.800-92.
20. Alaghbari K. A. et al. Complex Event Processing for Physical and Cyber Security in Datacentres: Recent Progress, Challenges and Recommendations. *Journal of Cloud Computing*. 2022. DOI: 10.1186/s13677-022-00338-x.
21. Valeur F., Vigna G., Kruegel C., Kemmerer R. A Comprehensive Approach to Intrusion Detection Alert Correlation. *IEEE Transactions on Dependable and Secure Computing*. 2004. Vol. 1, no. 3. P. 146–169. DOI: 10.1109/TDSC.2004.21.
22. Ning P., Cui Y., Reeves D. S. Constructing Attack Scenarios through Correlation of Intrusion Alerts. *Proceedings of the 9th ACM Conference on Computer and Communications Security*. 2002. P. 245–254. DOI: 10.1145/586110.586144.
23. Julisch K. Clustering Intrusion Detection Alarms to Support Root Cause Analysis. *ACM Transactions on Information and System Security*. 2003. Vol. 6, no. 4. P. 443–471. DOI: 10.1145/950191.950192.
24. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey. *ACM Computing Surveys*. 2009. Vol. 41, no. 3. Article 15. DOI: 10.1145/1541880.1541882.
25. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST

Special Publication 800-61 Revision 3. National Institute of Standards and Technology, 2025. DOI: 10.6028/NIST.SP.800-61r3.

26. Попов О., Драгунцов Р. Ключові виклики для операційних центрів кібербезпеки в умовах повномасштабної війни. Інформаційні технології та суспільство. 2025. № 3(18). С. 136–146. DOI: 10.32689/maup.it.2025.3.19.
27. Lipscombe P. Ukrainian telco Kyivstar to deploy more generators in fight against blackouts. Data Center Dynamics. URL: <https://www.datacenterdynamics.com/en/news/ukrainian-telco-kyivstar-to-deploy-more-generators-in-fight-against-blackouts> (дата звернення: 31.08.2025).
28. Зубок В. Ю., Драгунцов Р. І. Особливості розслідування та реагування на інциденти кібербезпеки в умовах масових відключень електропостачання. Безпека енергетики в епоху цифрової трансформації: матеріали V наук.-практ. конф., м. Київ, 22 листопада 2023 р. Київ, 2023.
29. Драгунцов Р. І. Алгоритм управління ризиками кібербезпеки в умовах знищення енергетичної інфраструктури. Кібербезпека енергетики: матеріали наук.-практ. конф., м. Київ, 28 травня 2025 р. Київ, 2025.
30. Lokot T. Russia's Networked Authoritarianism in Ukraine's Occupied Territories during the Full-Scale Invasion: Control and Resilience. PPR. URL: <https://ppr.lse.ac.uk/articles/10.31389/lseppr.85> (дата звернення: 31.08.2025).
31. Ukraine–Russia internet takeover. Wired. URL: <https://www.wired.com/story/ukraine-russia-internet-takeover> (дата звернення: 31.08.2025).
32. Ukraine's cyber specialists disrupt Russian industry backbone. Global Defence Technology. URL: https://defence.nridigital.com/global_defence_technology_aug24/latest-news-ukraine_war_dominant_in_cyber_operations (дата звернення: 31.08.2025).
33. Кадрова криза в Україні: брак спеціалістів. РБК-Україна. URL: <https://www.rbc.ua/rus/news/kadrova-kriza-ukrayini-k-brak-spetsialistiv-1727103044.html> (дата звернення: 31.08.2025).
34. Microsoft Digital Defense Report 2024. Microsoft, 2024. URL: <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf> (дата звернення: 31.08.2025).
35. Israel stage 3 cyber wars with Iran proxies. Dark Reading. URL: <https://www.darkreading.com/threat-intelligence/israel-stage-3-cyber-wars-with-iran-proxies> (дата звернення: 31.08.2025).
36. Petermann T., Bradke H., Lüllmann A., Poetzch M., Riehm U. What happens during a blackout. Technology Assessment Studies Series. Vol. 4. Norderstedt: BoD – Books on Demand, 2011.
37. Драгунцов Р.І., Зубок В.Ю. Динамічні інфраструктурні компоненти та видимість системи під час реагування на інциденти кібербезпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2025. №. 1(29). Р. 493–507. DOI: 10.28925/2663-4023.2025.29.891.
38. Skopik F., Landauer M., Wurzenberger M. Blind Spots of Security Monitoring in Enterprise Infrastructures: A Survey. IEEE Security & Privacy. 2022. Vol. 20, no. 6. Р. 18–26. DOI: 10.1109/MSEC.2021.3133764.
39. Noeparast E. B., Ravanmehr R. A Novel Event-Oriented Architecture for Logging and Auditing in Distributed Systems. Advances in Network and Communications. 2012. Vol. 1, no. 1. Р. 36–44. DOI: 10.4156/anc.vol1.issue1.4.

40. Li H., Li Y. LogSpy: System Log Anomaly Detection for Distributed Systems. 2020 International Conference on Artificial Intelligence and Computer Engineering (ICAICE), 23–25 October 2020. IEEE, 2020. P. 347–352. DOI: 10.1109/ICAICE51518.2020.00073.S
41. Siles S. Real world ARP spoofing. GIAC. URL: <https://www.giac.org/paper/gcih/487/real-world-arp-spoofing/105411> (дата звернення: 30.09.2024).
42. Kapade P., Pandey A. K. Technical issues and challenges in memory forensics. International Journal of Creative Research Thoughts (IJCRT). 2018. Vol. 6, issue 2.
43. Paar K., Harper S. Challenges and Mitigations for Data Remanance in FPGA Based Systems. 2024 NDIA Michigan Chapter Ground Vehicle Systems Engineering and Technology Symposium, Novi, Michigan, USA, 13 August 2024. DOI: 10.4271/2024-01-4112.
44. Lost site-to-site VPN connection after power outage. Check Point CheckMates. URL: <https://community.checkpoint.com/t5/SMB-Gateways-Spark/Lost-Site-to-Site-VPN-Connection-after-power-outage/td-p/215653> (дата звернення: 30.09.2024).
45. Buquerin K. K. G., Corbett C., Hof H.-J. Structured methodology and survey to evaluate data completeness in automotive digital forensics. 19th escar Europe – The World's Leading Automotive Cyber Security Conference, Ruhr region, Germany, 28 September 2021.
46. Драгунцов Р.І., Зубок В.Ю. Моделювання загроз кібербезпеці у зв'язку з масовими відключеннями електропостачання та потенційні заходи протидії. Електронне моделювання. 2023. Vol. 45, no. 3. P. 116–128. DOI: 10.15407/emodel.45.03.116.
47. Khan R., McLaughlin K., Laverty D., Sezer S. STRIDE-based threat modeling for cyber-physical systems. 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Torino, 26–29 September 2017. IEEE, 2018. DOI: 10.1109/ISGTEurope.2017.8260283.
48. Zografopoulos I., Ospina J., Liu X., Konstantinou C. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. IEEE Access. 2021. Vol. 9. P. 29775–29818. DOI: 10.1109/ACCESS.2021.3058403.
49. Flå L. H. Threat Modeling Framework for Smart Grids: master's thesis. Trondheim: Norwegian University of Science and Technology, 2021. 90 p. URL: <https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2781029/no.ntnu:inspera:66462738:38097967.pdf?sequence=1> (дата звернення: 15.05.2023).
50. Muckin M., Fitch S. C. A Threat-Driven Approach to Cyber Security: Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization. Lockheed Martin Corporation, 2019. 45 p. URL: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf> (дата звернення: 15.05.2023).
51. Using a Reserve Power Architecture to Increase Data Center Infrastructure Utilization and Efficiency. Columbus: Emerson Network Power Global Headquarters, 2014.
52. Petermann, T., Bradke, H., Lüllmann, A., Poetzch, M., & Riehm, U. (2011). What happens during a blackout (Technology Assessment Studies Series – 4). BoD – Books on Demand.
53. Business Continuity Management for SMEs using the Cloud. Bonn: Federal Office for Information Security, 2013.
54. Abualkishik A. Z., Alwan A. A., Gulzar Y. Disaster Recovery in Cloud Computing Systems: An Overview. International Journal of Advanced Computer Science and Applications. 2020. Vol. 11, no. 9. DOI: 10.14569/IJACSA.2020.0110984. URL: https://www.researchgate.net/publication/344435966_Disaster_Recovery_in_Cloud_Computing_Systems_An_Overview (дата звернення: 02.05.2026).

55. Ganesan P. Cloud-Based Disaster Recovery: Reducing Risk and Improving Continuity. *Journal of Artificial Intelligence & Cloud Computing*. 2024. Vol. 3, no. 1. P. 1–4. DOI: 10.47363/JAICC/2024(3)E162. URL: https://www.researchgate.net/publication/384389222_Cloud-Based_Disaster_Recovery_Reducing_Risk_and_Improving_Continuity (дата звернення: 02.05.2026).
56. Azodolmolky S., Wieder P., Yahyapour R. Cloud Computing Networking: Challenges and Opportunities for Innovations. *IEEE Communications Magazine*. 2013. Vol. 51, no. 7. P. 54–62. DOI: 10.1109/MCOM.2013.6553678. URL: https://www.researchgate.net/publication/249325475_Cloud_Computing_Networking_Challenges_and_Opportunities_for_Innovations (дата звернення: 02.07.2026)
57. Moura J., Hutchison D. Review and Analysis of Networking Challenges in Cloud Computing. *Journal of Network and Computer Applications*. 2016. Vol. 60. P. 113–129. DOI: 10.1016/j.jnca.2015.11.015.
58. Драгунцов Р.І., Зубок В.Ю. Методи підтримки спостережності інформаційно-комунікаційної інфраструктури в умовах повномасштабної війни. *Електронне Моделювання*. 2026. Vol. 48, no. 1. P. 72–86. DOI: 10.15407/emodel.48.01.072.
59. Burrell D. N. An Exploration of the Cybersecurity Workforce Shortage. *Cyber Warfare and Terrorism*. [S. l.]: IGI Global, 2020. P. 1072–1081. DOI: 10.4018/978-1-7998-2466-4.ch063.
60. Stone M., Irrechukwu C., Perper H., Wynne D. IT Asset Management. NIST Special Publication 1800-5. Gaithersburg: National Institute of Standards and Technology, 2018. DOI: 10.6028/NIST.SP.1800-5. URL: <https://csrc.nist.gov/pubs/sp/1800/5/final> (дата звернення: 08.05.2026).
61. Khaleghi B., Khamis A., Karray F. Multisensor data fusion: A review of the state-of-the-art. *Information Fusion*. 2011.
62. Pöhler L., Schuba M., Höner T., Hack S., Neugebauer G. An Open-Source Approach to OT Asset Management in Industrial Environments. *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*. SCITEPRESS, 2024. P. 128–136. DOI: 10.5220/0012362200003648.
63. Martseniuk Y., Partyka A., Harasymchuk O., Cherevyk V., Dovzhenko N. Research of the Centralized Configuration Repository Efficiency for Secure Cloud Service Infrastructure Management. *Cybersecurity Providing in Information and Telecommunication Systems. CEUR Workshop Proceedings*. 2025. Vol. 3991. P. 260–274. URL: <https://ceur-ws.org/Vol-3991/paper19.pdf> (дата звернення: 08.05.2026).
64. Efthymiopoulos, M. P.,. A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*. 8(1). DOI: 10.1186/s13731-019-0105-z .
65. Драгунцов Р. І., Зубок В. Ю. Застосування великих мовних моделей для автоматичної ідентифікації окремих атрибутів поверхні атаки активів в кібербезпеці. ШІБ-2025: матеріали наук.-практ. конф. URL: <https://ipme.kiev.ua/konferencii/naukovo-praktichna-konferenciya-sib-2025/> (дата звернення: 24.02.2026).
66. Drahuntsov R., Zubok V. A method for reducing the uncertainty caused by a power outage during a cyber incident response. *CEUR Workshop Proceedings*. 2024. Vol. 3887. P. 226–236. URL: <https://ceur-ws.org/Vol-3887/paper20.pdf> (дата звернення: 24.02.2026).
67. Drahuntsov R., Symonov A., Potenko O., Dybach O., Zubok V. Cybersecurity monitoring during power outages: Use cases for enhanced infrastructure observability and potential

- implications for NPP combined events. Nuclear and Radiation Safety. 2025. No. 3(107). P. 17–29. DOI: 10.32918/nrs.2025.3(107).02.
68. Jalalvand F., Chhetri M. B., Nepal S., Paris C. Alert Prioritisation in Security Operations Centres: A Systematic Survey on Criteria and Methods. ACM Computing Surveys. 2024. DOI: 10.1145/3695462.
69. Abd Bahrim A. M., Mohamad Hata M., Allias N., Bolhan Z. H., Darus M., Kamarudin S. I. B. Mitigating Alert Fatigue in Security Information and Event Management (SIEM): Ensemble Machine Learning Integration with Elasticsearch Logstash and Kibana (ELK). JOIV: International Journal on Informatics Visualization. 2026. Vol. 10, no. 2. DOI: 10.62527/joiv.10.2.4738.
70. Perez F., Granger B. E., Hunter J. D. Python: An Ecosystem for Scientific Computing. Computing in Science & Engineering. 2011. Vol. 13, no. 2. P. 13–21. DOI: 10.1109/MCSE.2010.119.
71. Alahmadi B. A., Axon L., Martinovic I. 99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms. 31st USENIX Security Symposium (USENIX Security 22), Boston, MA, USA, 10–12 August 2022. USENIX Association, 2022. P. 2783–2800. URL: <https://www.usenix.org/conference/usenixsecurity22/presentation/alahmadi> (дата звернення: 08.05.2026).
72. Tariq S., Chhetri M. B., Nepal S., Paris C. Alert Fatigue in Security Operations Centres: Research Challenges and Opportunities. ACM Computing Surveys. 2025. Vol. 57, no. 9. DOI: 10.1145/3723158.
73. Shon H., Lee Y., Yoon M. Semi-Supervised Alert Filtering for Network Security. Electronics. 2023. Vol. 12, no. 23. Article 4755. DOI: 10.3390/electronics12234755.
74. Russian Cyber Operations. State Service of Special Communications and Information Protection of Ukraine. 2024. URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=68768> (дата звернення: 08.05.2026).
75. VULNERABILITY DETECTION AND CYBER INCIDENT/CYBER ATTACK RESPONSE SYSTEM. CYBER INCIDENT RESPONSE OPERATIONS CENTRE OF THE STATE CYBER PROTECTION CENTRE OF THE STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE, 2024. URL: <http://scpc.gov.ua/api/files/4560c0ba-c6c0-4935-b48d-0232dd659df3>.
76. Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape. Google Threat Analysis Group, Mandiant, Google Trust & Safety. 2023. URL: <https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/> (дата звернення: 08.05.2026).

ДОДАТОК А

Список публікацій здобувача

- [1] R. Drahuntsov and V. Zubok, “Modeling of cyber threats related to massive power outages and potential countermeasures,” *Elektronnoe Modelirovanie*, vol. 45, no. 3, pp. 116–128, 2023, doi: 10.15407/emodel.45.03.116.
- [2] R. Drahuntsov, A. Symonov, O. Potenko, O. Dybach, and V. Zubok, “Cybersecurity monitoring during power outages: Use cases for enhanced infrastructure observability and potential implications for NPP combined events,” *Nuclear and Radiation Safety*, no. 3(107), pp. 17–29, 2025, doi: 10.32918/nrs.2025.3(107).02.
- [3] R. Drahuntsov and V. Zubok, “Dynamic infrastructure components and system vulnerabilities in wartime conditions,” *Cybersecurity: Education, Science, Technique*, no. 1(29), pp. 493–507, 2025, doi: 10.28925/2663-4023.2025.29.891.
- [4] R. Drahuntsov and D. Rabchun, “Potential disguising attack vectors on security operations centers through the use of AI methods: Information analysis,” *Cybersecurity: Education, Science, Technique*, no. 2(14), pp. 6–14, 2021, doi: 10.28925/2663-4023.2021.14.614.
- [5] R. Drahuntsov, D. Rabchun, and Z. Brzhevska, “Architecture security principles of the Android operating system,” *Cybersecurity: Education, Science, Technique*, no. 2(8), pp. 49–60, 2020, doi: 10.28925/2663-4023.2020.8.4960.
- [6] O. Popov and R. Drahuntsov, “Ключові виклики для операційних центрів кібербезпеки в умовах повномасштабної війни,” *Information Technology and Society*, no. 3(18), 2025, doi: 10.32689/maup.it.2025.3.19.
- [7] R. Drahuntsov and V. Zubok, “Methods for maintaining the observability of information and communication infrastructure in conditions of full-scale war,” *Elektronnoe Modelirovanie*, vol. 48, no. 1, pp. 72–86, 2026, doi: 10.15407/emodel.48.01.072.
- [8] R. Drahuntsov and V. Zubok, “A method for reducing the uncertainty caused by a power outage during a cyber incident response,” in *CEUR Workshop Proc.*, vol. 3887, pp. 226–236, 2024. [Online]. Available: ceur-ws.org/Vol-3887/paper20.pdf. Accessed: Feb. 24, 2026.
- [9] V. Yu. Zubok and R. S. Drahuntsov, “Проекція принципів національної системи стійкості та резильєнтності критичної інформаційної інфраструктури,” in *Proc. Sci.-Pract. Conf. “Резильєнтність критичної інфраструктури – 2023”*, Kyiv, Ukraine, Jun. 21, 2023, pp. 104–108. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2023/06/Матеріали-конференції-Critical-Infrastructure-Resilience---2023.pdf. Accessed: Feb. 24, 2026.

[10] V. Yu. Zubok and R. S. Drahuntsov, “Особливості розслідування та реагування на інциденти кібербезпеки в умовах масових відключень електропостачання,” in *Proc. V Sci.-Pract. Conf. “Безпека енергетики в епоху цифрової трансформації” (БЕЕЦТ-2023)*, Kyiv, Ukraine, 2023, pp. 38–42. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2023/11/Матеріали-конференції-БЕЕЦТ-2023.pdf. Accessed: Feb. 24, 2026.

[11] R. Drahuntsov and V. Zubok, “Особливості атак з використанням соціального графу та підходи до захисту,” in *Proc. 2nd All-Ukrainian Sci.-Pract. Conf. “Theoretical and Applied Cybersecurity” (TACS-2024)*, Kyiv, Ukraine, 2024. [Online]. Available: is.ipt.kpi.ua/pdf/T24.pdf. Accessed: Feb. 24, 2026.

[12] V. V. Zubok, R. S. Drahuntsov, and V. Yu. Zubok, “Резильєнтність ERP-систем в умовах енергетичної кризи,” in *Proc. Sci.-Pract. Conf. “Кібербезпека енергетики”*, Kyiv, Ukraine, 2024, pp. 13–16. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2024/06/Матеріали-КБЕ-2024.pdf. Accessed: Feb. 24, 2026.

[13] R. I. Drahuntsov, “Особливості інцидентів інформаційної безпеки з залученням шкідливого ПЗ в умовах кібервійни – аналіз та реагування,” in *Proc. Conf. Materials (v.2)*, Kyiv, Ukraine, 2024, pp. 65–68. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2024/05/Матеріали-конференції-2024-v-2.pdf. Accessed: Feb. 24, 2026.

[14] R. I. Drahuntsov and V. Yu. Zubok, “Проблематика інтеграції джерел виявлення технічних вразливостей в розрізі підтримки кіберстійкості критичної інфраструктури,” in *Proc. XLIII Sci.-Tech. Conf. Young Scientists and Specialists (PIMEE NAS of Ukraine)*, Kyiv, Ukraine, May 14, 2025, pp. 29–31. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2025/05/Materialy-KMV-2025.pdf. Accessed: Feb. 24, 2026.

[15] R. I. Drahuntsov, “Алгоритм управління ризиками кібербезпеки в умовах знищення енергетичної інфраструктури,” in *Proc. Sci.-Pract. Conf. “Кібербезпека енергетики” (КБЕ-2025)*, Kyiv, Ukraine, 2025. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2025/05/Матеріали-КБЕ-2025-1.pdf. Accessed: Feb. 24, 2026.

[16] R. I. Drahuntsov, “Процедури threat hunting в сучасному SOC – ключові підходи та проблематика оцінки покриття,” in *Proc. Conf. “Цифрова трансформація кібербезпеки”*, pp. 40–42, 2025. [Online]. Available: duikt.edu.ua/uploads/p_2779_36484696.pdf. Accessed: Feb. 24, 2026.

[17] R. I. Drahuntsov and V. Yu. Zubok, “Застосування великих мовних моделей для автоматичної ідентифікації окремих атрибутів поверхні атаки активів в кібербезпеці,” in *Proc. Sci.-Pract. Conf. “ШИБ-2025”*. [Online]. Available: ipme.kiev.ua/konferencii/naukovo-praktichna-konferenciya-sib-2025/. Accessed: Feb. 24, 2026.

ДОДАТОК Б

Програмний код прототипу модулів обрахунку дескриптору загроз та динамізму

```
from __future__ import annotations

from typing import Any, Dict, List, Tuple
import psycopg2
from psycopg2.extras import Json, RealDictCursor

ROLE_TTP_MAP: Dict[str, Dict[str, List[str]]] = {
    "domain_controller": {
        "tactics": [
            "Credential Access",
            "Privilege Escalation",
            "Persistence",
            "Lateral Movement",
            "Defense Evasion",
        ],
        "techniques": [
            "Valid Accounts",
            "Kerberos Abuse",
            "Directory Replication Abuse",
            "Remote Services",
            "Group Policy Manipulation",
        ],
    },
    "jump_host": {
        "tactics": [
            "Initial Access",
            "Execution",
            "Lateral Movement",
            "Defense Evasion",
        ],
        "techniques": [
            "External Remote Services",
            "Valid Accounts",
            "Command and Scripting Interpreter",
            "Remote Services",
        ],
    },
    "web_server": {
        "tactics": [
            "Initial Access",
            "Execution",
            "Persistence",
            "Command and Control",
        ],
        "techniques": [
            "Exploit Public-Facing Application",
            "Web Shell",
            "Server-Side Execution",
            "Application Layer Protocol",
        ],
    },
    "app_server": {
        "tactics": [
```

```

        "Initial Access",
        "Execution",
        "Persistence",
        "Lateral Movement",
    ],
    "techniques": [
        "Exploit Public-Facing Application",
        "Command and Scripting Interpreter",
        "Remote Services",
        "Service Manipulation",
    ],
},
"db_server": {
    "tactics": [
        "Credential Access",
        "Collection",
        "Exfiltration",
        "Impact",
    ],
    "techniques": [
        "Valid Accounts",
        "Database Access Abuse",
        "Data Staged",
        "Exfiltration Over Application Protocol",
    ],
},
"file_server": {
    "tactics": [
        "Collection",
        "Exfiltration",
        "Impact",
        "Lateral Movement",
    ],
    "techniques": [
        "Archive Collected Data",
        "Data Staged",
        "Remote Services",
        "Exfiltration Over Application Protocol",
    ],
},
"router": {
    "tactics": [
        "Initial Access",
        "Defense Evasion",
        "Command and Control",
        "Impact",
    ],
    "techniques": [
        "Network Device Access",
        "Impair Defenses",
        "Traffic Manipulation",
        "Network Denial of Service",
    ],
},
"switch": {
    "tactics": [
        "Defense Evasion",
        "Impact",
        "Command and Control",
    ],
},

```

```

        "techniques": [
            "Traffic Manipulation",
            "Network Device Access",
            "Network Service Disruption",
        ],
    },
    "segment_beacon": {
        "tactics": [
            "Defense Evasion",
            "Impact",
        ],
        "techniques": [
            "Indicator Removal on Host",
            "Monitoring Disruption",
            "Network Service Disruption",
        ],
    },
    "user_ws": {
        "tactics": [
            "Initial Access",
            "Execution",
            "Credential Access",
            "Lateral Movement",
        ],
        "techniques": [
            "Phishing",
            "User Execution",
            "Valid Accounts",
            "Remote Services",
        ],
    },
    "security_tool": {
        "tactics": [
            "Defense Evasion",
            "Impact",
            "Persistence",
        ],
        "techniques": [
            "Impair Defenses",
            "Modify Authentication Process",
            "Service Manipulation",
        ],
    },
}

```

```

def clamp(value: float, low: float = 0.0, high: float = 1.0) ->
float:
    return max(low, min(high, value))

```

```

def bool_score(value: Any) -> float:
    return 1.0 if bool(value) else 0.0

```

```

def inverse_reserve_score(minutes: Any, good_threshold: int) ->
float:
    """
    1.0 = резервування відсутнє/слабке
    0.0 = резервування достатнє або краще за поріг
    """

```

```

"""
if minutes is None:
    return 1.0
try:
    m = max(0, int(minutes))
except (TypeError, ValueError):
    return 1.0
return 1.0 - clamp(m / float(good_threshold))

def get_role(asset: Dict[str, Any]) -> str:
    return (asset.get("role") or "").strip().lower()

def get_asset_class(asset: Dict[str, Any]) -> str:
    return (asset.get("asset_class") or "").strip().lower()

def get_geo(asset: Dict[str, Any]) -> str:
    return (asset.get("geo_affiliation") or "").strip().lower()

def get_response_capability(asset: Dict[str, Any]) -> Dict[str,
Any]:
    rc = asset.get("response_capability")
    return rc if isinstance(rc, dict) else {}

def topology_volatility(asset: Dict[str, Any]) -> float:
    role = get_role(asset)
    asset_class = get_asset_class(asset)

    if asset_class == "cloud_asset":
        return 0.95
    if role in {"user_ws"} or asset_class == "workstation":
        return 0.85
    if role in {"router", "switch", "segment_beacon"} or asset_class
in {"network_device", "segment_beacon"}:
        return 0.80
    if role in {"web_server", "app_server"}:
        return 0.55
    if role in {"db_server", "domain_controller", "file_server"}:
        return 0.30
    if role in {"jump_host"}:
        return 0.45
    return 0.50

def state_volatility(asset: Dict[str, Any]) -> float:
    role = get_role(asset)
    asset_class = get_asset_class(asset)

    if asset_class == "cloud_asset":
        return 0.95
    if role in {"router", "switch", "segment_beacon"} or asset_class
in {"network_device", "segment_beacon"}:
        return 0.85
    if role in {"user_ws"} or asset_class == "workstation":
        return 0.75
    if role in {"web_server", "app_server"}:

```

```

        return 0.60
    if role in {"jump_host"}:
        return 0.50
    if role in {"db_server", "domain_controller", "file_server"}:
        return 0.35
    return 0.45

def cloud_control_fragility(asset: Dict[str, Any]) -> float:
    return 0.60 if bool(asset.get("cloud_agent_present")) else 0.20

def compute_single_asset_dynamicity(asset: Dict[str, Any]) ->
Tuple[float, float, Dict[str, Any]]:
    """
    Повептае:
    - dynamicity_score
    - visibility_loss_score
    - explanation
    """
    requires_network =
bool(asset.get("requires_network_connectivity", True))

    power_fragility =
inverse_reserve_score(asset.get("power_backup_minutes"),
good_threshold=180)
    channel_fragility = 0.0 if not requires_network else
inverse_reserve_score(
        asset.get("channel_backup_minutes"), good_threshold=120
    )
    topo = topology_volatility(asset)
    state = state_volatility(asset)
    cloud_fragility = cloud_control_fragility(asset)

    dynamicity_score = clamp(
        0.28 * power_fragility
        + 0.22 * channel_fragility
        + 0.20 * topo
        + 0.20 * state
        + 0.10 * cloud_fragility
    )

    if requires_network:
        visibility_loss_score = clamp(
            0.70 * dynamicity_score
            + 0.20 * channel_fragility
            + 0.10 * power_fragility
        )
    else:
        visibility_loss_score = clamp(
            0.80 * dynamicity_score
            + 0.20 * power_fragility
        )

    explanation = {
        "formula": "0.28*power_fragility + 0.22*channel_fragility +
0.20*topology_volatility + 0.20*state_volatility +
0.10*cloud_control_fragility",
        "factors": {
            "power_fragility": round(power_fragility, 4),

```

```

        "channel_fragility": round(channel_fragility, 4),
        "topology_volatility": round(topo, 4),
        "state_volatility": round(state, 4),
        "cloud_control_fragility": round(cloud_fragility, 4),
    },
}
return round(dynamicity_score, 6), round(visibility_loss_score,
6), explanation

```

```

def exposure_score(asset: Dict[str, Any]) -> float:
    role = get_role(asset)
    geo = get_geo(asset)
    service_group = (asset.get("service_group") or
"").strip().lower()
    requires_network =
bool(asset.get("requires_network_connectivity", True))

```

```

    base_map = {
        "domain_controller": 0.75,
        "jump_host": 0.85,
        "web_server": 0.90,
        "app_server": 0.70,
        "db_server": 0.65,
        "file_server": 0.60,
        "router": 0.85,
        "switch": 0.60,
        "segment_beacon": 0.50,
        "user_ws": 0.55,
        "security_tool": 0.70,
    }
    base = base_map.get(role, 0.50)

```

```

    if "edge" in geo:
        base += 0.10
    elif "office" in geo:
        base += 0.05

```

```

    if service_group in {"identity", "management"}:
        base += 0.05

```

```

    if not requires_network:
        base -= 0.20

```

```

    return clamp(base)

```

```

def build_attack_vectors(asset: Dict[str, Any], exposure: float) -
> List[str]:
    role = get_role(asset)
    rc = get_response_capability(asset)
    vectors: List[str] = []

    if exposure >= 0.80:
        vectors.append("high_remote_exposure")
    elif exposure >= 0.60:
        vectors.append("moderate_remote_exposure")

    if role in {"domain_controller", "jump_host", "router",
"switch"}:

```

```

        vectors.append("privileged_infrastructure_role")

    if bool(asset.get("requires_network_connectivity", True)):
        vectors.append("network_dependency")

    if bool(asset.get("cloud_agent_present")):
        vectors.append("cloud_control_plane_dependency")

    if inverse_reserve_score(asset.get("power_backup_minutes"),
180) >= 0.80:
        vectors.append("low_power_reserve")

    if inverse_reserve_score(asset.get("channel_backup_minutes"),
120) >= 0.80:
        vectors.append("low_channel_reserve")

    if not bool(rc.get("edr_isolation", False)):
        vectors.append("limited_host_containment")

    if not bool(rc.get("fw_block", False)):
        vectors.append("limited_network_containment")

    return vectors[:20]

def observable_coverage_ratio(asset: Dict[str, Any]) -> float:
    """
    Апроксимація частки покриття релевантних технік.
    У поточній схемі немає матриці control->technique, тому
    використовуються проксі-ознаки.
    """
    asset_class = get_asset_class(asset)
    rc = get_response_capability(asset)

    edr_isolation = bool_score(rc.get("edr_isolation", False))
    fw_block = bool_score(rc.get("fw_block", False))
    cloud_agent = bool_score(asset.get("cloud_agent_present",
False))
    power_reserve = 1.0 -
inverse_reserve_score(asset.get("power_backup_minutes"), 60)
    channel_reserve = 1.0 -
inverse_reserve_score(asset.get("channel_backup_minutes"), 60)

    if asset_class in {"network_device", "segment_beacon"}:
        score = (
            0.20
            + 0.45 * fw_block
            + 0.10 * cloud_agent
            + 0.10 * power_reserve
            + 0.15 * channel_reserve
        )
    elif asset_class in {"server", "host", "workstation"}:
        score = (
            0.15
            + 0.30 * cloud_agent
            + 0.25 * edr_isolation
            + 0.15 * fw_block
            + 0.05 * power_reserve
            + 0.10 * channel_reserve
        )

```

```

elif asset_class == "cloud_asset":
    score = (
        0.20
        + 0.35 * cloud_agent
        + 0.20 * edr_isolation
        + 0.15 * fw_block
    )
else:
    score = (
        0.15
        + 0.25 * cloud_agent
        + 0.20 * edr_isolation
        + 0.20 * fw_block
    )

return round(clamp(score), 6)

def descriptor_confidence(asset: Dict[str, Any]) -> float:
    checks = [
        asset.get("asset_class") is not None,
        asset.get("role") is not None,
        asset.get("criticality") is not None,
        asset.get("power_backup_minutes") is not None,
        asset.get("channel_backup_minutes") is not None,
        isinstance(asset.get("response_capability"), dict),
        asset.get("geo_affiliation") is not None,
    ]
    return round(sum(1 for x in checks if x) / len(checks), 6)

def compute_single_asset_threat_descriptor(asset: Dict[str, Any]) -
> Tuple[Dict[str, Any], float]:
    role = get_role(asset)
    asset_class = get_asset_class(asset)
    criticality = float(asset.get("criticality") or 0.0)
    exposure = exposure_score(asset)
    coverage_ratio = observable_coverage_ratio(asset)

    mapped = ROLE_TTP_MAP.get(
        role,
        {
            "tactics": ["Discovery", "Defense Evasion"],
            "techniques": ["System Information Discovery", "Impair
Defenses"],
        },
    )

    attack_vectors = build_attack_vectors(asset, exposure)
    confidence = descriptor_confidence(asset)

    descriptor: Dict[str, Any] = {
        "schema_version": "threat_descriptor.v1",
        "asset_class": asset_class,
        "role": role,
        "criticality": round(criticality, 6),
        "exposure_score": round(exposure, 6),
        "observable_coverage_ratio": round(coverage_ratio, 6),
        "tactics": mapped["tactics"],
        "techniques": mapped["techniques"],
    }

```

```

        "attack_vectors": attack_vectors,
        "confidence": confidence,
        "rationale": (
            f"Descriptor is derived from role={role},
asset_class={asset_class}, "
            f"criticality={criticality:.3f},
exposure={exposure:.3f}, "
            f"coverage_ratio={coverage_ratio:.3f}."
        ),
    }

    th_priority_index = clamp(
        0.60 * criticality
        + 0.25 * exposure
        + 0.15 * (1.0 - coverage_ratio)
    )

    return descriptor, round(th_priority_index, 6)

def compute_and_update_dynamicity(conn:
psycopg2.extensions.connection) -> int:
    """
    Обчислює dynamicity_score і visibility_loss_score для всіх не-
retired активів
    та записує значення назад у sam_assets.
    """
    updated_rows = 0

    select_sql = """
        SELECT
            asset_id,
            asset_name,
            asset_class,
            role,
            segment_id,
            service_group,
            criticality,
            geo_affiliation,
            power_backup_minutes,
            channel_backup_minutes,
            cloud_agent_present,
            response_capability,
            requires_network_connectivity,
            status
        FROM sam_assets
        WHERE status <> 'retired'
        ORDER BY asset_name;
    """

    update_sql = """
        UPDATE sam_assets
        SET
            dynamicity_score = %s,
            visibility_loss_score = %s,
            updated_at = now()
        WHERE asset_id = %s;
    """

    with conn.cursor(cursor_factory=RealDictCursor) as cur:

```

```

        cur.execute(select_sql)
        assets = cur.fetchall()

        for asset in assets:
            dynamicity_score, visibility_loss_score, _ =
compute_single_asset_dynamics(asset)
            cur.execute(
                update_sql,
                (dynamicity_score, visibility_loss_score,
asset["asset_id"]),
            )
            updated_rows += 1

    conn.commit()
    return updated_rows

def compute_and_update_threat_descriptor(conn:
psycopg2.extensions.connection) -> int:
    """
    Обчислює threat_descriptor і th_priority_index для всіх не-
retired активів
    та записує значення назад у sam_assets.
    """
    updated_rows = 0

    select_sql = """
        SELECT
            asset_id,
            asset_name,
            asset_class,
            role,
            segment_id,
            service_group,
            criticality,
            geo_affiliation,
            power_backup_minutes,
            channel_backup_minutes,
            cloud_agent_present,
            response_capability,
            requires_network_connectivity,
            status
        FROM sam_assets
        WHERE status <> 'retired'
        ORDER BY asset_name;
    """

    update_sql = """
        UPDATE sam_assets
        SET
            threat_descriptor = %s,
            th_priority_index = %s,
            updated_at = now()
        WHERE asset_id = %s;
    """

    with conn.cursor(cursor_factory=RealDictCursor) as cur:
        cur.execute(select_sql)
        assets = cur.fetchall()

```

```

        for asset in assets:
            descriptor, th_priority_index =
compute_single_asset_threat_descriptor(asset)
            cur.execute(
                update_sql,
                (Json(descriptor), th_priority_index,
asset["asset_id"]),
            )
            updated_rows += 1

    conn.commit()
    return updated_rows

```