**УДК 004.056:004.89:623.746.4-519**

***Нехороших Дмитро Михайлович***

*асистент кафедри Безпеки інформаційних технологій*
*Харківський національний університет радіоелектроніки*

***Туз Михайло Олександрович***

*студент VI курсу Харківського*
*національного університету радіоелектроніки*

# РИЗИК-ОРІЄНТОВАНА МОДЕЛЬ ПОБУДОВИ ТА УПРАВЛІННЯ SOC НА ОСНОВІ ІНТЕГРОВАНОЇ АРХІТЕКТУРИ МОНІТОРИНГУ

**Анотація:** У роботі запропоновано ризик-орієнтовану модель побудови та управління операційним центром безпеки (Security Operations Center, SOC), яка поєднує бізнес-контекст, критичні активи, сценарії кіберризику, вимоги до виявлення, багатоджерельну телеметрію, централізовану аналітику SIEM та спеціалізовані засоби EDR/XDR/NDR. Обґрунтовано перехід від технологічно орієнтованої моделі SOC до моделі, у якій склад джерел моніторингу і сценарії виявлення визначаються ризиками. Запропоновано замкнений цикл SOC: від виявлення й розслідування до реагування, метрик, засвоєння уроків та переоцінювання ризиків.

**Ключові слова:** SOC, SIEM, EDR, XDR, NDR, телеметрія безпеки, кіберризик, моніторинг, виявлення, реагування на інциденти, кіберстійкість.

**Вступ**. Розвиток цифрової інфраструктури, використання хмарних сервісів, віддаленого доступу, гібридних середовищ і великої кількості спеціалізованих засобів захисту ускладнюють забезпечення безперервної видимості кіберзагроз. Операційний центр безпеки (SOC) за таких умов повинен розглядатися не як окремий інструмент або сукупність інформаційних панелей, а як організаційна спроможність, що поєднує персонал, процеси, дані, технології та механізми управління. У практиці побудови SOC поширеним залишається технологічно орієнтований підхід: спочатку впроваджуються SIEM, EDR, NDR або інші платформи, після чого організація намагається пристосувати до них процеси моніторингу. Такий підхід може призводити до надлишкового збору подій, значної кількості хибнопозитивних спрацювань, прогалин видимості та слабкого зв'язку між технічними сигналами і реальними бізнес-ризиками.

Актуальність ризик-орієнтованого підходу підтверджується сучасними рамковими документами. NIST Cybersecurity Framework 2.0 розглядає функції: КЕРУВАТИ, ВИЗНАЧАТИ, ЗАХИЩАТИ, ВИЯВИТИ, РЕАГУВАТИ ТА ВІДНОВЛЯТИ (GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND і RECOVER) як взаємопов'язані результати управління кіберризиками [1]. NIST SP 800-61 Rev. 3 додатково інтегрує реагування на інциденти у ширший процес управління кіберризиками і підкреслює необхідність постійного вдосконалення можливостей виявлення, реагування та відновлення. [2]. ENISA визначає SOC як функцію, що забезпечує виявлення інцидентів шляхом спостереження за технічними подіями мереж і систем та може бути залучена до реагування й оброблення інцидентів [3].

**Мета доповіді.** Запропонувати узагальнену ризик-орієнтовану модель побудови та управління SOC, яка пов'язує бізнес-контекст і кіберризики з вимогами до виявлення, складом телеметрії безпеки,

архітектурою SIEM/EDR/XDR/NDR, процесами розслідування та реагування, а також механізмами зворотного зв'язку для постійного вдосконалення системи управління інформаційною безпекою.

Вихідним принципом запропонованої моделі є відмова від побудови SOC «від інструментів». Першим рівнем є бізнес-контекст: критичні процеси, інформаційні активи, сервіси, технологічні залежності та прийнятний рівень ризику. На їх основі формуються сценарії кіберризику. Для кожного суттєвого сценарію визначається вимога до виявлення (Detection Requirement), тобто перелік спостережуваних ознак, які дозволяють своєчасно встановити факт реалізації загрози. Таким чином встановлюється послідовність: «актив → ризик → сценарій атаки → вимога до виявлення → необхідна телеметрія».

Цей підхід змінює логіку журналювання та збору даних. Телеметрія безпеки повинна формуватися не за принципом максимально можливого накопичення журналів, а відповідно до конкретних Detection Use Cases. Наприклад, для сценарію компрометації привілейованого облікового запису необхідно поєднати дані автентифікації та MFA, зміни привілеїв, поведінку кінцевої точки, мережеві з'єднання і, за наявності, хмарну активність. Відсутність одного з ключових джерел може створити прогалину видимості навіть за формально справної SIEM.

Другий рівень моделі утворює операційний контур SOC, який охоплює технології, джерела телеметрії, аналітичні механізми та процеси реагування. Усередині цього контуру взаємодіють Endpoint/EDR, Identity/IAM, Network/NDR, Cloud/SaaS, Email Security, XDR, прикладні системи, Threat Intelligence, дані про активи й уразливості та SIEM. SIEM у такій архітектурі є центральним механізмом централізації, нормалізації, кореляції та пошуку подій із різних джерел, але не ототожнюється із самим SOC. SOC є ширшою організаційно-операційною спроможністю, яка охоплює моніторинг, виявлення, сортування, розслідування, управління

випадками/інцидентами, реагування, відновлення, звітування та постійне вдосконалення (monitoring, detection, triage, investigation, case/incident management, response, recovery, reporting і continual improvement). Зовнішнім щодо операційного контуру залишається управлінський рівень: бізнес-контекст, критичні активи, кіберризики та вимоги до виявлення, які визначають пріоритети моніторингу і необхідний склад телеметрії.

Третій рівень моделі – керований телеметричний конвеєр. Дані проходять етапи збору, передавання, синтаксичного розбору (Parsing), нормалізації (Normalization), збагачення (Enrichment), зберігання та аналітики. Помилка на будь-якому з цих етапів безпосередньо впливає на якість detection. Наприклад, несправний колектор створює blind spot, неправильний parser не заповнює потрібні поля, а застарілий контекст активу знижує якість пріоритезації. Тому показники «стан джерел даних, охоплення телеметрією та якість даних» (Data Source Health, Telemetry Coverage та Data Quality) повинні входити до системи операційного контролю SOC нарівні з alert- та incident-метриками.

Четвертий рівень – архітектура виявлення. Окреме правило виявлення (Detection Rule) є лише технічною реалізацією ширшого сценарію виявлення (Detection Use Case). Повноцінний Use Case повинен включати пов'язаний ризиковий сценарій, необхідну телеметрію, логіку виявлення, тяжкість (Severity), контекст активу і користувача, власника, порядок реагування, критерії тестування, tuning та метрики. Для систематизації поведінки противника доцільно використовувати MITRE ATT&CK, яка надає базу реальних тактик і технік та дозволяє співвідносити Detection Use Cases з конкретними TTP [4].

П'ятий рівень – операційний цикл SOC. Виявлена активність проходить послідовність «Сповіщення → Сортування → Розслідування → Визначення масштабів → Прийняття рішення → Справа/Інцидент → Ескалація → Реагування → Відновлення → Закриття». Такий підхід

принципово відрізняється від спрощеної моделі «logs → SIEM → alert», оскільки центром операційної діяльності стає не сам факт спрацювання правила, а кероване прийняття рішення з урахуванням критичності активу, потенційного бізнес-впливу, контексту загроз та вразливостей. Можна сформулювати так:

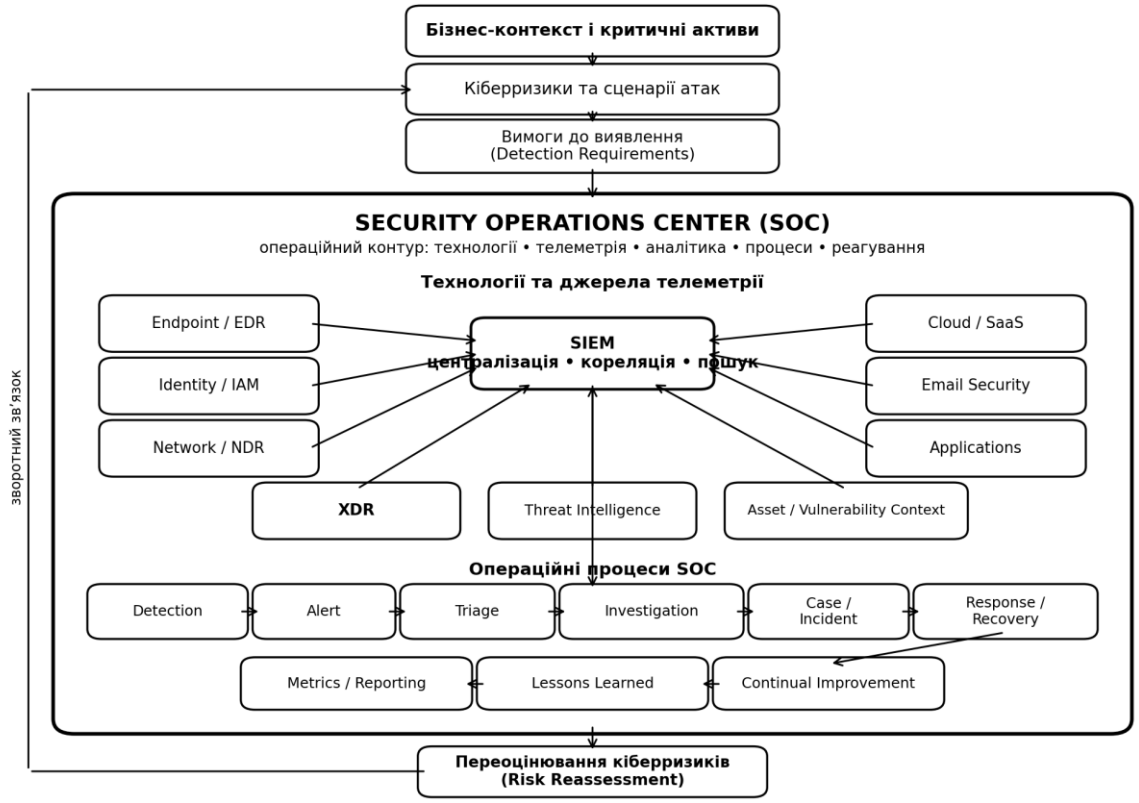


*Рис. 1. Ризик-орієнтована модель побудови та управління SOC*

Управління справами (Case Management) при цьому забезпечує визначення відповідальних, дотримання встановлених строків реагування (SLA), збереження доказів, ведення журналу аудиту та передачу справ між змінами, а оркестрація, автоматизація та реагування у сфері безпеки (SOAR) може автоматизувати збагачення даних, перевірку індикаторів компрометації (IOC), створення справ і виконання дозволених дій реагування лише після формалізації відповідного процесу.

Запропонована модель передбачає, що операційна модель SOC має

бути надбудовою над технологічною архітектурою. Вона визначає ролі та компетенції персоналу, повноваження щодо прийняття рішень, порядок ескалації, угоди про рівень обслуговування (SLA) та операційний рівень взаємодії (OLA), режим роботи 8×5 або 24×7, правила передачі інформації між змінами, внутрішню, зовнішню або гібридну модель організації SOC, а також взаємодію з командами реагування на інциденти, експлуатації IT-інфраструктури, інженерії безпеки, управління, ризиків і відповідності вимогам (GRC), юридичного супроводу та забезпечення безперервності бізнесу. ENISA зазначає, що показники діяльності SOC мають охоплювати швидкість і повноту виявлення, рівень покриття моніторингом, частку хибнопозитивних спрацювань, кількість оброблених інцидентів, співвідношення подій, сповіщень та інцидентів, кількість ескалацій і рівень робочого навантаження [3].

Це підтверджує необхідність вимірювати не продуктивність окремого продукту, а операційну спроможність SOC.

Ключовою відмінністю запропонованої моделі є замкнений контур зворотного зв'язкуПісля завершення інциденту результати розслідування, показники ефективності та отримані уроки мають використовуватися для виявлення прогалин у системі виявлення та захисних заходах, уточнення вимог до телеметрії, налаштування правил виявлення, удосконалення засобів захисту та переоцінювання кіберризиків.

Після цього оновлені risk scenarios знову формують вимоги до виявлення. Такий цикл відповідає логіці постійного вдосконалення й забезпечує інтеграцію Security Operations із ISMS та управлінням кіберризиками.

Запропонований підхід також безпосередньо пов'язаний з кіберстійкістю. Здатність організації протистояти сучасним загрозам визначається не лише превентивними controls, а й можливістю швидко побачити аномальну активність, зрозуміти її контекст, локалізувати вплив,

відновити роботу і адаптувати захист. ENISA Threat Landscape 2025 характеризує сучасне середовище як таке, що потребує intelligence-driven і systemic defensive strategies, поведінкового виявлення, proactive threat hunting та інтеграції cyber risk management у ширші операційні процеси [5].

**Висновки.** Ризик-орієнтована модель побудови SOC дозволяє перейти від технологічно орієнтованої архітектури до capability-oriented підходу, у якому склад засобів моніторингу, телеметрії та Detection Use Cases визначається критичними активами і сценаріями кіберризику. SIEM у такій моделі є центральним аналітичним шаром, EDR/XDR/NDR та інші засоби – спеціалізованими джерелами detection і response, а SOC Operating Model забезпечує кероване перетворення технічних сигналів на рішення та дії. Замикання циклу через metrics, lessons learned і risk reassessment створює основу для постійного вдосконалення SOC та підвищення кіберстійкості організації.

## Список використаних джерел

1. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg : National Institute of Standards and Technology, 2024. NIST CSWP 29. DOI: https://doi.org/10.6028/NIST.CSWP.29.
2. Nelson A., Rekhi S., Scarfone K., Souppaya M. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. Gaithersburg : National Institute of Standards and Technology, 2025. NIST SP 800-61 Rev. 3. DOI: https://doi.org/10.6028/NIST.SP.800-61r3.
3. European Union Agency for Cybersecurity. How to set up CSIRT and SOC. Heraklion : ENISA, 2020. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20How%20to%20setup%20CSIRT%20and%20SOC.pdf.
4. MITRE ATT&CK. Enterprise Matrix. URL: https://attack.mitre.org/matrices/enterprise/.
5. European Union Agency for Cybersecurity. ENISA Threat Landscape 2025. Heraklion : ENISA, 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.
6. European Union Agency for Cybersecurity. Guideline on Security Measures under the EECC. 4th ed. Heraklion : ENISA, 2021. URL:

https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc.