DOI: 10.18372/2225-5036.31.21161

МЕТОДИКА КЕРУВАННЯ ЯКІСТЮ АЛЕРТІВ У SIEM НА ОСНОВІ РИЗИК-ОРІЄНТОВАНОГО СКОРИНГУ ТА ЗВОРОТНОГО ЗВ'ЯЗКУ SOC (ALERT QUALITY MANAGEMENT)

Юлія Костюк, Павло Складанний, Світлана Рзаєва

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

КОСТЮК Юлія Володимирівна, Phd in Computer Science
Рік та місце народження: 1980 рік, м. Київ, Україна
Освіта: Державний торговельно-економічний університет.
Посада: доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Наукові інтереси: захист інформації, комп'ютерні мережі, інформаційно-комунікаційні системи, інформаційно-інтелектуальні системи, нейронні мережі.
Публікації: більше 100 наукових публікацій, серед яких монографія, посібник, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: y.kostiuk@kubg.edu.ua
Orcid ID: 0000-0001-5423-0985.

СКЛАДАННИЙ Павло Миколайович, кандидат технічних наук, доцент,
Рік та місце народження: 1992 рік, м. Київ, Україна
Освіта: Державний університет телекомунікацій.
Посада: завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Наукові інтереси: кібербезпека, криптографія, криптоаналіз, математичне моделювання.
Публікації: більше 100 наукових публікацій, серед яких монографії, підручники, посібники, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: p.skladannyi@kubg.edu.ua
Orcid ID: 0000-0002-7775-6039.

РЗАЄВА Світлана Леонідівна, кандидат технічних наук, доцент
Освіта: Севастопольський приладобудівний інститут.
Рік та місце народження: 1968 рік, м. Київ, Україна
Посада: доцент кафедри кафедри комп'ютерних наук
Наукові інтереси: адміністрування і захист баз даних та сховищ даних, моделювання програмного забезпечення та його аналіз, інформаційні технології та системи
Публікації: більше 100 наукових публікацій, серед яких монографії, підручники, посібники, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: s.rzaieva@kubg.edu,ua
Orcid ID: 0000-0002-7589-2045.

Анотація. *У роботі розроблено методику керування якістю алертів у системах управління подіями та інцидентами інформаційної безпеки (SIEM) на основі ризик-орієнтованого скорингу та замкненого контуру зворотного зв'язку від Security Operations Centre. Актуальність дослідження зумовлена проблемою перевантаження аналітиків SOC надмірною кількістю сповіщень, значна частина яких має низьку аналітичну цінність і не призводить до підтверджених інцидентів безпеки. На відміну від підходів, що зосереджуються переважно на вдосконаленні кореляції подій або підвищенні точності детекції, запропонована методика розглядає алерт як керований операційний об'єкт і формалізує його якість через інтегральний показник Alert Quality Index (AQI). Даний показник враховує корисність алерта для реагування, часову релевантність його обробки, рівень дублювання сповіщень та витрати аналітичних ресурсів SOC. Ризик-скоринг алертів коригується з урахуванням критичності активів, ролей користувачів і загрозового контексту, що забезпечує узгодження технічних сигналів SIEM з потенційним впливом інцидентів на бізнес-процеси підприємства. Для зменшення alert flood у роботі застосовано механізми дедуплікації та зшивання однотипних сповіщень у більш інформативні кейси на основі метрики подібності в заданому часовому вікні. Рішення аналітиків SOC (TP, FP, BENIGN, TUNE) використовуються як керуючий сигнал для адаптивного тюнінгу порогових значень і параметрів правил SIEM. Експериментальна перевірка у серії номінальних і стресових сценаріїв продемонструвала зниження частки хибнопозитивних спрацювань, скорочення MTTD і MTTR, зменшення навантаження на SOC та зростання середнього значення AQI, що підтверджує ефективність системного керування потоком алертів у реальних умовах експлуатації.*

Ключові слова: *SIEM, SOC, alert fatigue, керування якістю алертів, ризик-орієнтований скоринг, інциденти безпеки, дедуплікація, зворотний зв'язок.*

Постановка проблеми

Сучасні системи управління подіями та інцидентами інформаційної безпеки (SIEM) є ключовим елементом інфраструктури кіберзахисту підприємства, забезпечуючи централізований збір, аналіз і виявлення потенційно небезпечних подій [1, 6]. Проте на практиці ефективність SIEM значною мірою обмежується не можливостями збору або кореляції подій, а якістю сформованих алертів та здатністю команди SOC ефективно з ними працювати.

У реальних умовах експлуатації SIEM-системи генерують значну кількість алертів, значна частина яких має низьку аналітичну цінність, дублює одна одну або не призводить до підтверджених інцидентів безпеки [3, 11]. Така ситуація призводить до явища alert fatigue — перевантаження аналітиків SOC надмірною кількістю сповіщень, що знижує уважність, збільшує час реагування та підвищує ризик пропуску дійсно критичних загроз. У результаті навіть коректно налаштована SIEM може демонструвати незадовільні експлуатаційні показники.

Більшість наявних підходів до вдосконалення роботи SIEM зосереджуються на розвитку механізмів кореляції подій, розширенні правил виявлення або застосуванні методів машинного навчання [7, 17]. Водночас питання керування якістю алертів як самостійного об'єкта дослідження залишається недостатньо формалізованим [1-3]. У наукових і прикладних роботах, як правило, оцінюється кількість виявлених інцидентів або точність детекції, але не аналізується повний життєвий цикл алерта — від моменту його формування до підтвердження, ескалації або закриття.

На практиці алерт є не просто технічним результатом спрацювання правила, а операційною одиницею взаємодії між SIEM і командою SOC, яка безпосередньо впливає на ключові показники ефективності: середній час виявлення (MTTD), середній час реагування (MTTR), частку хибнопозитивних спрацювань (False Positive Rate), навантаження аналітиків, дотримання SLA реагування та загальний рівень ризику для підприємства [1-2, 6]. Відсутність формалізованих критеріїв якості алертів унеможливлює системне порівняння різних конфігурацій SIEM і обґрунтований тюнінг правил виявлення.

Окремою проблемою є те, що більшість SIEM-систем використовують фіксовані або напівстатичні порогові значення для формування алертів, які не враховують контекст активів, критичність бізнес-процесів, історичну "корисність" алертів і фактичний досвід роботи аналітиків SOC [11]. У результаті тюнінг правил часто виконується вручну, реактивно та фрагментарно, без формалізованого зворотного зв'язку та кількісного підтвердження покращень.

Таким чином, виникає науково-прикладна проблема розроблення методики керування якістю алертів у SIEM, яка б дозволяла:

- кількісно оцінювати якість сформованих алертів;
- ранжувати алерти за рівнем ризику з урахуванням контексту активів і загроз;
- зменшувати рівень алерт-флуду та дублювання сповіщень без втрати здатності виявляти критичні інциденти;
- забезпечувати адаптивний тюнінг правил на основі фактичного зворотного зв'язку від SOC;
- об'єктивно оцінювати вплив запропонованих змін на KPI ефективності SIEM.

Розв'язання цієї проблеми потребує переходу від локальної оптимізації окремих правил до системного підходу керування алертами, у якому алерт розглядається як вимірюваний, ризик-орієнтований і керований об'єкт у межах процесів SOC. Саме це зумовлює актуальність розроблення методики Alert Quality Management, спрямованої на підвищення експлуатаційної ефективності SIEM-систем у реальних умовах функціонування підприємства.

Наукова новизна дослідження полягає у розробленні та обґрунтуванні методики керування якістю алертів у SIEM-системах, яка розглядає алерт не як побічний результат спрацювання правила виявлення, а як керований об'єкт у межах процесів SOC із формалізованими характеристиками якості, ризику та операційної доцільності. На відміну від наявних підходів, зосереджених переважно на кореляції подій або підвищенні точності детекції, запропонована методика орієнтована на системне управління життєвим циклом алертів та їхній вплив на ключові показники ефективності SIEM.

Вперше запропоновано формалізований показник якості алертів (Alert Quality Index, AQI), який інтегрує не лише класичні метрики точності виявлення, а й операційні характеристики обробки алертів у SOC, зокрема рівень дублювання, часові затримки підтвердження, фактичну корисність алертів для реагування та витрати аналітичних ресурсів. Такий підхід дозволяє кількісно оцінювати якість потоку алертів і використовувати цю оцінку як керуючий параметр для тюнінгу SIEM.

Отримав подальший розвиток підхід до ризик-орієнтованої пріоритезації алертів, у межах якого ризик-скоринг формується з урахуванням критичності активів, контексту користувачів і поведінкових ознак, що забезпечує узгодження технічних сигналів SIEM з реальним впливом потенційних інцидентів на бізнес-процеси підприємства [10, 19]. На відміну від традиційної пріоритезації за статичними правилами, запропонований підхід дозволяє динамічно адаптувати пріоритети алертів відповідно до контексту експлуатації.

Уперше в межах методики Alert Quality Management сформовано замкнений контур зворотного зв'язку SOC, у якому результати аналізу алертів (підтверджені інциденти, хибнопозитивні спрацювання, безпечні події, потреба в тюнінгу)

використовуються як керуючий сигнал для адаптивного коригування порогових значень і параметрів формування алертів [21]. Це забезпечує перехід від реактивного ручного тюнінгу до керованого та відтворюваного процесу оптимізації якості алертів.

Практична цінність і наукова новизна методики підтверджуються експериментальною перевіркою впливу керування якістю алертів на ключові KPI SIEM, зокрема MTTD, MTTR, частку хибнопозитивних алертів і навантаження аналітиків SOC. Отримані результати демонструють, що підвищення ефективності SIEM може бути досягнуте не шляхом ускладнення кореляційних моделей, а за рахунок системного управління якістю алертів та використання зворотного зв'язку від операційних процесів SOC.

Аналіз останніх досліджень і публікацій

Останні дослідження свідчать, що ключовою практичною проблемою функціонування SIEM/SOC є не стільки сам факт виявлення подій безпеки, скільки керування якістю потоку алертів, що включає зменшення шуму, уникнення дублювання, коректну пріоритезацію сповіщень і підтримання стабільних показників ефективності, таких як MTTD, MTTR, частка хибнопозитивних спрацювань та навантаження на аналітиків SOC. У фокусі сучасної наукової літератури перебуває явище alert fatigue — виснаження персоналу SOC через надлишкову кількість алертів, яке безпосередньо погіршує швидкість і точність триажу, підвищує ризик пропуску реальних інцидентів і формує критичне «вузьке місце» в процесах реагування. Узагальнюючий огляд цієї проблематики, поданий у роботі Tariq et al. [1], систематизує основні причини виникнення alert fatigue та підкреслює обмеження наявних підходів: навіть за умов застосування методів машинного навчання й автоматизації вирішальними залишаються питання якості сигналу, пояснюваності пріоритетів і організації структурованого зворотного зв'язку від аналітиків.

Паралельно формується окремий науковий напрям, присвячений пріоритезації алертів у Security Operations Centre як самостійній задачі управління. У систематичному огляді Jalalvand et al. [2] показано, що ефективна пріоритезація має враховувати не лише технічну «підозрілість» події, а й контекст її виникнення, зокрема критичність активу, роль користувача, важливість сервісу та потенційний вплив на бізнес-процеси [11, 19]. Саме поєднання технічних і контекстних факторів визначає реальну пріоритетність реагування та дозволяє зменшити навантаження на SOC без втрати здатності виявляти критичні загрози. Водночас дослідження Landauer et al. [3] демонструє, що навіть у суміжних доменах, таких як антивірусні та EDR-алерти, пріоритезація й агрегація дають відчутний ефект лише за наявності формалізованої оцінки корисності алерта та механізмів зменшення надлишкових спрацьовувань.

Значний інтерес викликають масштабовані підходи до триажу та фільтрації алертів, спрямовані на зменшення обсягу ручної роботи аналітиків SOC. Зокрема, у роботі Oliver et al. [4] запропоновано метод реального часу для триажу алертів на основі великомасштабного кластерування та швидкого пошуку, який дозволяє суттєво підвищити співвідношення «signal-to-noise» шляхом відокремлення типових хибних тригерів від підозрілих контекстів. Подібну спрямованість має й підхід Turcotte et al. [5], у якому розглядаються інтелектуальні системи автоматизованої класифікації та пріоритезації алертів, що навчаються на результатах попереднього аналізу SOC. Водночас автори підкреслюють необхідність контрольованого використання таких рішень, оскільки відсутність чітко визначених ризикових порогів і керованого зворотного зв'язку може призводити до накопичення прихованих помилок.

На рівні SIEM-платформ і методів оброблення даних активно обговорюються підходи до збору, нормалізації та аналітики подій, а також застосування принципів машинного навчання в SIEM-пайплайнах [6-7, 17]. Разом із тим наголошується, що без системного керування якістю алертів, яке включає дедуплікацію, тюнінг правил, контроль частки хибнопозитивних спрацювань і вплив на SLA реагування, навіть потужні аналітичні механізми можуть призводити до перевантаження SOC та зниження операційної ефективності [15, 21]. Оглядові публікації також фіксують зсув від суто технологічного опису SIEM до управлінського виміру, орієнтованого на показники ефективності, витрати обробки подій і узгодження процесів моніторингу з цілями підприємства.

Отже, за результатами аналізу сучасних публікацій можна зробити висновок, що наукова і практична увага поступово зміщується до задач Alert Quality Management, зокрема формалізації якості алертів, ризик-орієнтованої пріоритезації та побудови замкненого контуру «SOC feedback → тюнінг правил і порогів» [1-2, 4-5]. Як підкреслюється у працях [6-8], ефективність SIEM у реальних умовах визначається не кількістю виявлених подій, а здатністю системи зменшувати шум, керувати хибнопозитивними спрацюваннями та підтримувати стабільні операційні показники SOC. Водночас у наявній літературі все ще бракує цілісної методики, яка б одночасно задавала формальні показники якості алертів, визначала ризик-скоринг з урахуванням критичності активів і контексту та використовувала структурований зворотний зв'язок SOC як керуючий сигнал для оптимізації FPR, навантаження аналітиків, MTTD та MTTR. Саме ця прогалина обґрунтовує необхідність розроблення методики керування якістю алертів у SIEM без повторення кореляційних моделей, але з прямим виходом на вимірюваний вплив на KPI та процеси SOC.

Мета та постановка завдання

Метою даного дослідження є розроблення та експериментальна перевірка методики керування якістю алертів у SIEM-системах, що ґрунтується на ризик-орієнтованому скорингу та використанні зворотного зв'язку від команди SOC з метою підвищення експлуатаційної ефективності

моніторингу безпеки, зменшення рівня алерт-флуду та оптимізації навантаження на аналітиків [1-3, 21]. Досягнення цієї мети передбачає перехід від традиційного підходу, орієнтованого на кількість згенерованих сповіщень або формальну точність правил виявлення, до системного управління життєвим циклом алертів, у межах якого кожен алерт розглядається як керований об'єкт із вимірюваними характеристиками якості, ризику та операційної доцільності для процесів реагування.

Для реалізації поставленої мети у роботі здійснюється аналіз життєвого циклу алертів у SIEM-системах та визначаються ключові фактори, що впливають на їхню якість, зокрема рівень дублювання сповіщень, частка хибнопозитивних алертів, часові затримки їх обробки та залежність ефективності реагування від контексту активів і користувачів [1-3, 11, 21]. На основі цього пропонується формалізований показник якості алертів — Alert Quality Index, який інтегрує метрики точності детекції, операційні характеристики обробки та фактичну корисність алертів для прийняття рішень у SOC [19]. Паралельно розробляється модель ризик-орієнтованого скорингу алертів, що враховує критичність активів, контекст ролей користувачів, поведінкові ознаки та типові сценарії загроз, забезпечуючи пріоритезацію сповіщень відповідно до потенційного впливу на підприємство.

З метою зменшення шуму та підвищення інформативності сповіщень у методиці передбачається застосування алгоритмів дедуплікації та зшивання алертів у кейси, що дозволяє скоротити кількість однотипних алертів без втрати здатності виявляти критичні інциденти безпеки. Важливим елементом запропонованого підходу є контур зворотного зв'язку від команди SOC, у межах якого результати обробки алертів — підтвердження, хибні спрацювання, безпечні події або потреба в тюнінгу — використовуються для автоматизованого або напівавтоматизованого коригування порогових значень і параметрів формування алертів. Такий підхід забезпечує адаптивність SIEM-системи до змін у середовищі загроз і накопиченого експлуатаційного досвіду.

Запропонована методика проходить експериментальну перевірку на практичному стенді SIEM із використанням типових сценаріїв атак і use-case, з фіксацією показників ефективності до та після її впровадження. Оцінювання результатів здійснюється за ключовими показниками ефективності, зокрема середнім часом виявлення та реагування, часткою хибнопозитивних алертів, навантаженням аналітиків SOC і дотриманням SLA реагування. У підсумку розв'язання поставлених завдань дозволяє сформувати формалізовану та практично перевірену методику Alert Quality Management, придатну для використання в SIEM-системах різного класу та спрямовану на підвищення стійкості й керованості процесів моніторингу та реагування на інциденти інформаційної безпеки в умовах реальної експлуатації.

Методи дослідження включають: нормалізацію та інтеграцію різнорідних ознак алертів; ризик-скоринг на основі логістичної моделі з контекстною корекцією; побудову метрики подібності для дедуплікації; експериментальне порівняння режимів "до/після" впровадження Alert Quality Management; оцінювання ефективності за KPI MTTD, MTTR, FPR, навантаження SOC та середнім AQI.

Обмеження застосовності методики пов'язані з якістю контекстних даних (CMDB/IDM/CTI) та наявністю процедур фіксації рішень SOC (міток TP/FP/BENIGN/TUNE). На етапі "cold start" (відсутність історичних міток) AQI більше спирається на ризик-орієнтовані компоненти та експертні ваги; у подальшому, за накопичення даних, перевага надається емпіричній корисності алертів для SOC.

Виклад основного матеріалу дослідження

Запропонована методика керування якістю алертів у SIEM-системах ґрунтується на розгляді алерта як самостійного керованого об'єкта, що має вимірювані характеристики якості, ризику та операційної доцільності для процесів Security Operations Centre [1-2, 21]. На відміну від традиційного підходу, у якому алерт є кінцевим результатом спрацювання правила або моделі детекції, у межах методики Alert Quality Management алерт розглядається як елемент замкненого керуючого контуру, що безпосередньо впливає на ефективність реагування та навантаження аналітиків SOC.

Рис. 1. ілюструє замкнений керуючий контур, у якому результати роботи Security Operations Centre використовуються для адаптивного налаштування параметрів SIEM. Схема відображає системний характер методики та взаємодію її основних компонентів. SIEM формує алерти, які разом із контекстною інформацією передаються до модуля Alert Quality Management (AQM) для оцінювання ризику та якості на основі показників Risk Score і Alert Quality Index (AQI). Пріоритезовані алерти або кейси надходять до SOC для тріажу, за результатами якого формується структурований зворотний зв'язок у вигляді міток TP, FP або TUNE. Отриманий зворотний зв'язок використовується як керуючий сигнал для коригування порогів, ваг скорингу та параметрів правил SIEM, що забезпечує безперервне покращення якості алертів і стабілізацію ключових показників реагування відповідно до вимог ISO/IEC 27001.

Методика орієнтована на керування потоком алертів, а не на локальну оптимізацію окремих правил виявлення. Її основна ідея полягає у тому, що навіть коректно налаштовані механізми детекції можуть призводити до деградації показників SIEM за відсутності системного підходу до оцінювання та регулювання якості алертів у процесі експлуатації. Тому керування якістю алертів здійснюється на рівні всього їх життєвого циклу — від моменту формування до остаточного рішення SOC.

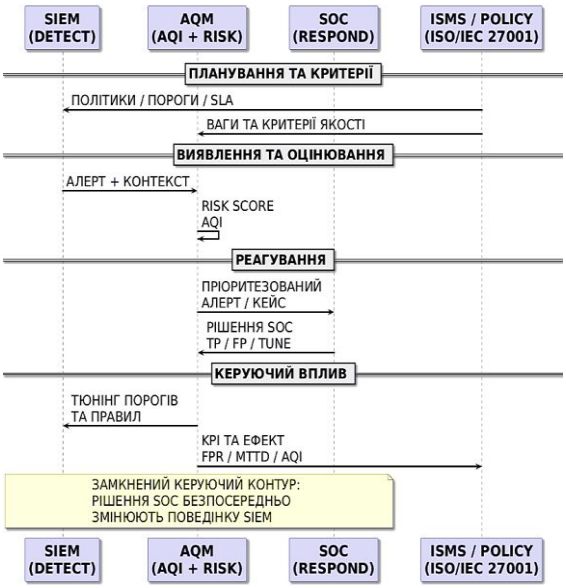

Рис. 1. Концептуальна схема Alert Quality Management у SIEM

У межах запропонованої методики життєвий цикл алерта включає такі основні етапи: формування алерта на основі подій безпеки, попередню нормалізацію та збагачення контекстом, оцінювання якості й ризику алерта, дедуплікацію та зшивання однотипних сповіщень, пріоритезацію для обробки SOC, прийняття рішення аналітиком та фіксацію результату у вигляді структурованого зворотного зв'язку. Кожен з цих етапів розглядається як точка впливу на загальну якість потоку алертів.

Рис. 2. Життєвий цикл алерта як керованого об'єкта

На рис. 2 наведено життєвий цикл алерта як керованого об'єкта з розподілом функцій між SIEM, модулем Alert Quality Management (AQM) та Security Operations Centre (SOC). Схема відображає послідовність перетворення алерта від моменту надходження подій безпеки до формування керуючих дій, що впливають на подальші параметри моніторингу. На рівні SIEM здійснюється збір подій безпеки та формування алертів, які слугують вхідними об'єктами для подальшої обробки. У межах AQM алерти проходять нормалізацію та збагачення контекстом, після чого для них обчислюється ризик-орієнтований скоринг і показник якості AQI, що забезпечує кількісну оцінку їх операційної корисності [11, 19, 23]. Подальшим етапом є дедуплікація та зшивання однотипних алертів у кейси, які передаються до SOC для тріажу та аналітичної перевірки [23]. За результатами аналізу формуються рішення TP, FP, BENIGN або TUNE, які фіксуються у вигляді структурованого зворотного зв'язку. Отриманий зворотний зв'язок використовується в AQM для формування керуючих дій — коригування порогів, ваг скорингу та параметрів правил SIEM [18, 23-24]. Таким чином реалізується замкнений контур керування, у якому якість алертів розглядається як керований ресурс, а досвід SOC використовується для безперервного покращення процесів виявлення та реагування.

Ключовим елементом методики є оцінювання якості алертів за допомогою інтегрального показника Alert Quality Index (AQI). AQI відображає не лише формальну точність виявлення, а й операційну корисність алерта для SOC, зокрема його унікальність, часову релевантність, історичну ймовірність підтвердження інциденту та витрати аналітичного ресурсу на його обробку [23]. Таким чином, якість алерта визначається не за внутрішніми характеристиками правила, а за фактичним внеском алерта у процес реагування.

Паралельно в методиці використовується ризик-орієнтований скоринг алертів (Risk-Alert Score), який забезпечує їх ранжування з урахуванням контексту активів, ролей користувачів і потенційного впливу на бізнес-процеси підприємства [10, 18-19, 24]. Ризик-скоринг дозволяє узгодити технічні сигнали SIEM з рівнем допустимого ризику та критичністю інформаційних ресурсів, забезпечуючи пріоритетну обробку тих алертів, які можуть мати найбільші наслідки у разі підтвердження інциденту.

Для зменшення алерт-флуду та дублювання сповіщень у методиці передбачено застосування алгоритмів дедуплікації та зшивання алертів у кейси, які об'єднують однотипні або логічно пов'язані алерти в межах заданого часового вікна та контексту [1-5, 14, 23]. Це дозволяє суттєво скоротити кількість одиниць, що потребують ручної обробки, без втрати інформації про розвиток потенційного інциденту.

Принциповою відмінністю запропонованої методики є наявність замкненого контуру зворотного

зв'язку від SOC, у якому результати аналізу алертів фіксуються у стандартизованому вигляді (підтверджений інцидент, хибнопозитивне спрацювання, безпечна подія, потреба в тюнінгу) [1-2, 21, 24]. Цей зворотний зв'язок використовується як керуючий сигнал для адаптивного коригування порогових значень, вагових коефіцієнтів скорингу та параметрів формування алертів, що забезпечує поступове підвищення їх якості в процесі експлуатації SIEM.

Таким чином, запропонована методика керування якістю алертів формує системний підхід до оптимізації роботи SIEM [9], у якому зменшення шуму, підвищення точності реагування та стабілізація ключових KPI досягаються не за рахунок ускладнення детекційних моделей, а через кероване використання ризик-орієнтованого скорингу та експлуатаційного досвіду SOC.

У межах методики Alert Quality Management формалізація спрямована на перехід від інтуїтивного або фрагментарного тюнінгу правил до відтворюваного, кількісно вимірюваного та керованого процесу обробки алертів у SIEM [1-2, 9]. Для цього алерт розглядається не як кінцевий технічний результат спрацювання правила, а як операційний об'єкт із формалізованими характеристиками якості та ризику, що безпосередньо впливають на навантаження аналітиків і ефективність реагування SOC. У межах такого підходу вводяться інтегральний показник якості алерта Alert Quality Index (AQI), ризик-орієнтований скоринг Risk-Alert Score, правила дедуплікації та зшивання алертів у кейси, а також замкнений контур зворотного зв'язку SOC, який коригує параметри правил, порогів і ваг скорингу на основі фактичних рішень аналітиків.

Базовими об'єктами формалізації є алерт і кейс. Алерт трактується як повідомлення SIEM про потенційно небезпечну подію або шаблон подій, сформоване правилом чи детектором, тоді як кейс визначається як агрегований об'єкт, що об'єднує групу однотипних або логічно пов'язаних алертів у межах заданого часового вікна [9, 14]. Процедура дедуплікації розглядається як механізм зменшення алерт-флуду шляхом об'єднання алертів із високою подібністю за ключовими полями, контекстними ознаками та часовою близькістю, що дозволяє скоротити кількість одиниць ручної обробки без втрати інформації про розвиток інциденту.

Кількісна оцінка ризику та якості алертів базується на формуванні вектора ознак $x(a)$, який узагальнює технічні, контекстні та поведінкові характеристики події [7, 11, 19]. Формування цього вектора здійснюється на основі нормалізованих полів алерта SIEM, зокрема ідентифікатора правила, рівня критичності, тегів use-case або MITRE ATT&CK, мережевих атрибутів та часових характеристик, а також результатів збагачення контекстом за рахунок даних розвідки загроз (CTI), репутаційних індикаторів і політик доступу [12-13, 20]. Додатково використовуються дані підприємства, зокрема інформація з CMDB або каталогу сервісів для оцінювання критичності активів Crit(asset), дані систем керування ідентифікацією та доступом для визначення ролей користувачів $Role_u$, а також профілі джерел телеметрії для оцінки довіри до детекторів Conf(src) [16, 18]. Для узгодженого поєднання різнорідних показників усі ознаки приводяться до інтервалу [0,1] шляхом лінійної або експоненційної нормалізації залежно від типу метрики, що забезпечує коректну подальшу інтеграцію в ризик-скоринг і показник якості.

На основі сформованого вектора ознак і контекстних параметрів далі вводяться формальні залежності для обчислення ризик-орієнтованого скорингу, інтегрального індексу якості алерта та керуючих правил дедуплікації й тюнінгу [16], що дозволяє кількісно описати весь життєвий цикл алерта — від моменту формування до використання рішень SOC як керуючого сигналу для оптимізації параметрів SIEM.

Нехай SIEM формує множину алертів $A = \{a_1, \dots a_N\}$ [6-7, 15]. Для кожного алерта ааа визначається вектор контексту та ознак:

$$x(a) = [x_1(a), x_2(a), \dots, x_m(a)],\ x_k(a) \in [0,1], \quad (1)$$

де $x(a)$ − нормалізований набір ознак алерта, що може включати, наприклад: технічну "підозрілість" події, аномальність, індикатори відповідності use-case, ознаки збагачення CTI, атрибути активу та користувача [2, 7, 19]. Нормалізація до $[0,1]$ потрібна для узгодженого поєднання різнорідних метрик у подальших індексах.

Також задається контекст підприємства:

- $Crit(asset) \in [0,1]$ − критичність активу (сервісу/хоста/даних);
- $Role(u) \in [0,1]$ − вагова оцінка ролі/привілеїв користувача;
- $Conf(src) \in [0,1]$ − довіра до джерела/детектора (sensor confidence);
- $Threat(t) \in [0,1]$ − оцінка рівня загрозового контексту (напр., за CTI).

Ці величини отримуються з CMDB/IDM/каталогу сервісів/політики ризику та можуть бути задані як експертно, так і за шкалами підприємства.

Ризик-скоринг алерта використовується для пріоритезації черги SOC та ранжування сповіщень за очікуваним впливом. Введемо функцію [11, 21]:

$$R(a) = \sigma(\beta_0 + \sum_{k=1}^{m} \beta_k\, x_k(a)),\ \delta(z) = \frac{1}{1+e^{-z}}. \quad (2)$$

де $R(a) \in [0,1]$ — ризик-оцінка алерта, β_0 — зсув (базовий рівень ризику), β_k — ваги ознак $x_k(a)$, які задаються експертно або калібруються на історії SOC, $\delta(\cdot)$ — логістична функція, що забезпечує коректне обмеження результату в $[0,1]$.

Щоб ризик враховував критичність активу і контекст, вводиться мультиплікативна корекція:

$$R_{ctx}(a) = 1 - (1 - R(a)) \cdot (1 - Crit(asset(a))) \cdot (1 - Role(u(a))) \cdot (1 - Threat(t(a))), \quad (3)$$

Формула (3) інтерпретується як "ймовірність того, що алерт є критичним з урахуванням контексту": якщо хоча б один фактор (актив/роль/загроза) високий, то $R_{ctx}(a)$ зростає навіть за помірної технічної підозрілості [11, 19, 21]. Така агрегація зручна тим, що не "занижує" ризик при високій критичності активів. $R_{ctx}(a)$ визначає первинний пріоритет у черзі SOC, пороги ескалації та політики реакції (наприклад, автоматична ізоляція або вимога додаткових перевірок).

На рис. 3 наведено структуру ризик-орієнтованого скорингу алерта, подану у вигляді діаграми активності, що відображає послідовність формування ризику як керованого показника. Процес розпочинається з отримання множини ознак алерта $x(a)$, які характеризують зафіксовану подію безпеки та слугують вхідними даними для подальшого аналізу. На наступному етапі на основі логістичної моделі обчислюється базовий ризик $R(a)$, що відображає технічну ймовірність небезпечності події без урахування операційного контексту. Далі ризик послідовно коригується з урахуванням критичності задіяного активу, ролі користувача та актуального загрозового контексту, що забезпечує інтеграцію бізнес- і середовищних факторів у процес оцінювання. Завершальним етапом є формування контекстно-орієнтованого ризику $R_{ctx}(a)$, який використовується для подальших рішень щодо пріоритезації, фільтрації та обробки алертів у SOC. Таким чином, схема візуально підкреслює, що ризик-орієнтований скоринг виходить за межі простого anomaly score та реалізує керований процес оцінювання з урахуванням контексту експлуатації.

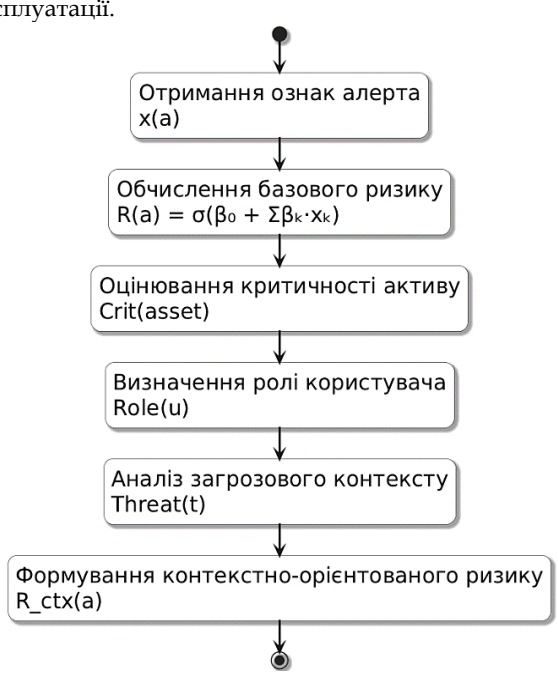

Рис. 3. Структура ризик-орієнтованого скорингу алерта

Якість алерта в методиці визначається не лише ризиком, а й тим, наскільки алерт "корисний" у реальній роботі SOC. Для цього вводяться операційні величини [1-2, 21]:

- $\tau_{ack}(a)$ – час до першого підтвердження/прийняття в роботу (acknowledgement);
- $\tau_{close}(a)$ – час до закриття алерта (закрито/ескаловано/передано);
- $d(a) \in [0,1]$ – коефіцієнт дублювання (чим ближче до 1, тим більш дубльований алерт);
- $c(a) \in [0,1]$ – "вартість обробки" (оцінка витрат часу/ресурсів SOC);
- $y(a) \in \{0,1\}$ – результат розмітки SOC: 1 – алерт призвів до підтвердженого інциденту або корисної ескалації; 0 – хибнопозитивний/безпечний.

Для нормування часових показників використовується шкала:

$$T_{ack}(a) = exp\left(-\frac{\tau_{ack}(a)}{\theta_{ack}}\right),\ T_{close}(a) = exp\left(-\frac{\tau_{close}(a)}{\theta_{close}}\right), \quad (4)$$

де $\theta_{ack}, \theta_{close} > -$ параметри нормування, які задаються відповідно до SLA/політики SOC. Експоненційна форма означає: що швидше оброблено алерт, то більша "операційна релевантність" (наближається до 1), а при великих затримках — швидко спадає.

Введемо інтегральний показник якості алерта:

$$AQI(a) = w_1 \cdot U(a) + w_2 \cdot T_{ack}(a) + w_3 \cdot T_{close}(a) + w_4 \cdot \big(1 - d(a)\big) - w_5 \cdot c(a), \quad (5)$$

де $w_i \geq 0, \sum_{i=1}^{5} w_i = 1$ — ваги, що задають пріоритети підприємства (наприклад, що важливіше: швидкість чи зменшення дублювання). Компоненти формули: $U(a) \in [0,1]$ – корисність алерта для SOC, $T_{ack}(a), T_{close}(a)$ — нормовані часові показники (4), $\big(1 - d(a)\big)$ — штраф за дублювання, $c(a)$ — штраф за "дорогі" в обробці алерти.

Корисність алерта визначається як поєднання фактичного результату SOC та ризикового контексту:

$$U(a) = \alpha \cdot y(a) + (1 - \alpha) \cdot R_{ctx}(a), \alpha \in [0,1], \quad (6)$$

де α задає баланс між "історичною істинністю" (мітками SOC) і ризиком за контекстом. Якщо історичних даних мало, α зменшують, щоб система не переобтяжувалась шумними оцінками; якщо даних достатньо — α збільшують, роблячи AQI більш "емпіричним".

Для того щоб індекс був у межах [0,1], застосовується відсікання:

$$AQI^*(a) = \min\{1, \max\{0, AQI(a)\}\}, \quad (7)$$

$AQI^*(a)$ застосовується для оцінювання якості потоку алертів у SIEM "до/після" тюнінгу, для порівняння конфігурацій правил та як керуючий сигнал при автоматизованому налаштуванні порогів.

Дедуплікація спрямована на зменшення алерт-флуду шляхом об'єднання однотипних алертів в межах короткого інтервалу часу. Для двох алертів a_i та a_j вводиться функція подібності [1-4, 13]:

$$S(a_i, a_j) = \lambda_1 \cdot S_{key}(a_i, a_j) + \lambda_2 \cdot S_{ctx}(a_i, a_j) + \lambda_3 \cdot S_{time}(a_i, a_j), \quad (8)$$

де $\lambda_k \geq 0, \sum_{k=1}^{3} \lambda_k = 1$, S_{key} — збіг ключових полів (rule id, tactic/technique tag, signature, dst/src), S_{ctx} — збіг

контексту (asset, user, service, segment/VLAN), S_{time} — часовий фактор, наприклад [3-4]:

$$S_{time}(a_i, a_j) = \exp\left(-\frac{|t_i - t_j|}{\Delta t}\right), \quad (9)$$

де t_i, t_j — часи появи алертів, Δt — ширина часового вікна для оцінювання подібності та зшивання алертів.

Правило дедуплікації:

$$\text{якщо } S(a_i, a_j) \geq \theta_{dup} \text{ тоді } a_i \sim a_j \text{ (належать одному кластеру/кейсу)}, \quad (10)$$

де $\theta_{dup} \in [0,1]$ — поріг подібності, вище якого алерти об'єднуються в один кластер/кейс. На практиці його вибір визначає компроміс між зменшенням шуму та ризиком "склеїти" різні події.

Кожному кластеру (кейсу) C ставиться у відповідність агрегований алерт [4-5]:

$$a_C = Aggregate(C), \quad (11)$$

де оператор $Aggregate(C)$, формує:

- часовий інтервал кейсу $[t_{min}, t_{max}]$,
- кількість злитих алертів $|C|$,
- представницький контекст (asset/user/service),
- максимальний або середній ризик $R_{ctx}(a)$ по кластеру,
- пояснювальну інформацію для SOC (які алерти були об'єднані і чому).

Дедуплікація зменшує кількість одиниць обробки у черзі SOC, а "кейс" стає більш інформативним об'єктом для триажу та ескалації.

На рис. 4 наведено графову інтерпретацію процесу дедуплікації алертів у SIEM на основі метрики подібності. Окремі алерти aia_iai подані у вигляді вершин графа, а наявність ребра між парою алертів означає виконання умови подібності $S(a_i, a_j) \geq \theta_{dup}$. Алерти, що утворюють зв'язну компоненту графа, об'єднуються в кластер C, який інтерпретується як логічно пов'язана група однотипних сповіщень. Для кожного кластера формується агрегований кейс $a_C = Aggregate(C)$, що узагальнює часові межі $[t_{min}, t_{max}]$, кількість об'єднаних алертів $|C|$ та ризикові характеристики (зокрема максимальне або середнє значення R_{ctx}). Сформовані кейси надходять до черги SOC замість окремих алертів, що дозволяє суттєво зменшити кількість одиниць ручної обробки при одночасному збереженні та збагаченні контекстної інформації для аналітиків.

Нехай кожен алерт після обробки SOC отримує мітку:

$$\ell(a) \in \{TP, FP, BENIGN, TUNE\}, \quad (12)$$

де TP — підтверджена загроза/інцидент, FP — хибнопозитивний алерт, $BENIGN$ — безпечна подія (не загроза), $TUNE$ — потребує коригування правила/порогів/винятків.

Для кожного правила/детектора rrr на часовому інтервалі W збираються підсумкові статистики [1-2, 9]:

$$FP_{rate}(r) = \frac{N_{FP}(r)}{N_{all}(r)}, TP_{rate}(r) = \frac{N_{TP}(r)}{N_{all}(r)}, \quad (13)$$

де W — інтервал накопичення статистик для тюнінгу, $N_{all}(r)$ — кількість алертів, породжених правилом r у вікні W.

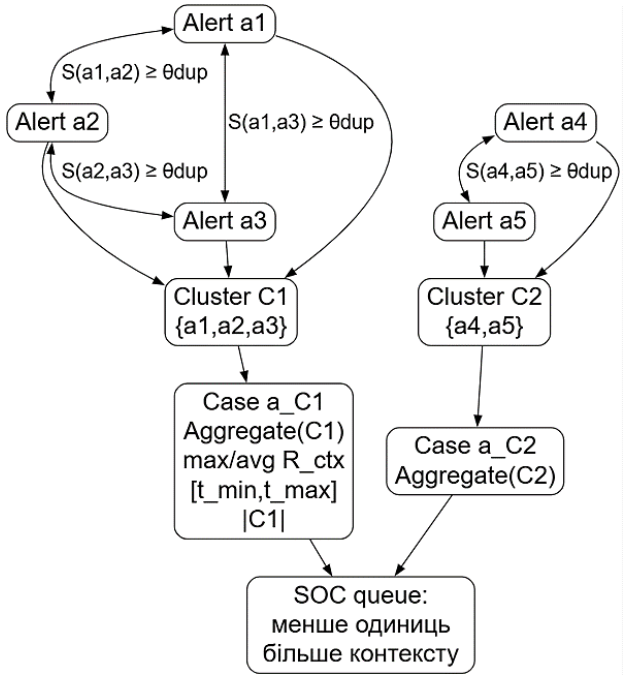

Рис. 4. Графова модель дедуплікації та зшивання алертів у кейси

Далі вводиться керуючий закон зміни порогу правила r (або ваги ознаки), що зменшує FP при збереженні здатності фіксувати критичні події [9]:

$$\theta_r^{(t+1)} = \theta_r^{(t)} + \eta \cdot (FP_{rate}(r) - \rho) - \mu \cdot (TP_{rate}(r) - k), \quad (14)$$

де θ_r — поріг спрацювання правила/детектора r $\theta_r^{(t)}$ — поточний поріг спрацювання правила, $\eta > 0$ — крок реакції на хибнопозитивні, $\mu > 0$ — крок "утримання" здатності детекції, ρ — допустимий рівень FP (policy threshold), k — мінімально прийнятний рівень TP.

Якщо правило дає FP вище допустимого рівня ρ, поріг збільшується (спрацьовувань стає менше), а якщо при цьому падає TP нижче k, поріг зменшується, щоб не втрачати важливі алерти. Таким чином реалізується керований компроміс між шумом і чутливістю.

Для відбору правил, які потребують першочергового тюнінгу, формується пріоритет тюнінгу [9]:

$$P_{tune}(r) = \gamma_1 \cdot FP_{rate}(r) + \gamma_2 \cdot \bar{c}(r) + \gamma_3 \cdot (1 - \overline{AQI^*}(r)), \quad (15)$$

де $\bar{c}(r)$ та $\overline{AQI^*}(r)$ — середні значення вартості та якості алертів, породжених правилом r у вікні W. Високе $P_{tune}(r)$ означає: правило створює шум, дорого обробляється та має низьку якість — отже, воно є пріоритетним кандидатом на корекцію.

Формули (12)–(15) реалізують замкнений контур "SOC feedback → тюнінг", який перетворює накопичений досвід аналітиків на формальні керуючі дії для підвищення якості потоку алертів.

Для кількісного підтвердження ефекту методики у розділі експерименту оцінюються [1-2, 21-22]:

• MTTD — середній час виявлення/потрапляння в роботу;

• MTTR — середній час реагування/закриття;

• FPR — частка хибнопозитивних алертів;

• L — навантаження на SOC (кількість алертів/кейсів на зміну або за інтервал);

• $\overline{AQI^*}(r)$ — середня якість алертів до/після тюнінгу.

Саме ці показники використовуються для порівняння конфігурацій "до/після" та для обґрунтування того, що підвищення ефективності SIEM досягається системним керуванням якістю алертів, а не лише ускладненням детекційних механізмів.

На рис. 5 наведено замкнений контур зворотного зв'язку між SOC і SIEM, у межах якого результати аналізу алертів (мітки TP, FP, BENIGN, TUNE) агрегуються за правилами та використовуються як керуючий сигнал для адаптивного оновлення порогів θ_r. Оновлені параметри впливають на подальше формування алертів, що забезпечує безперервне зменшення хибнопозитивних спрацювань і відрізняє запропоновану методику від класичного статичного налаштування SIEM.

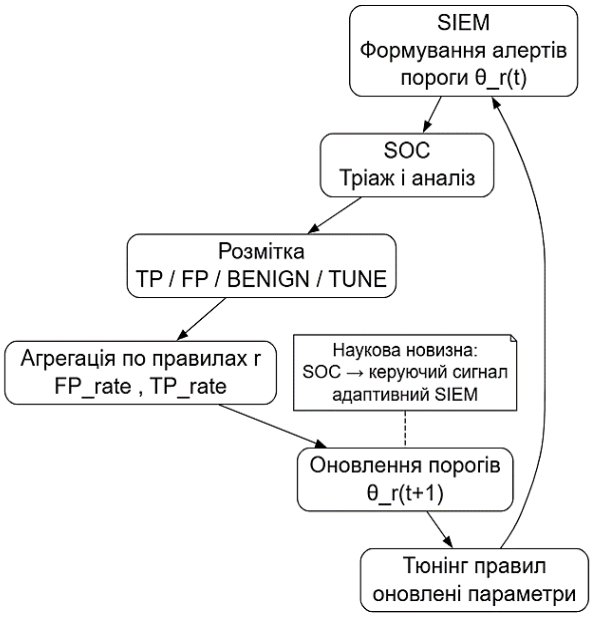

Рис. 5. Замкнений контур зворотного зв'язку SOC

Експериментальну перевірку запропонованої методики виконано в умовах, наближених до типового функціонування SIEM у складі процесів Security Operations Centre підприємства, коли потік подій безпеки надходить із різнорідних джерел, нормалізується та збагачується контекстом, після чого на його основі формуються алерти, що проходять триаж і прийняття рішень аналітиками [9, 18]. Для порівняння розглядалися два режими роботи: базовий, у якому алерти формуються за фіксованими порогами та правилами з переважно ручним реактивним налаштуванням, і режим із впровадженням Alert Quality Management, де застосовано ризик-орієнтований скоринг, інтегральний показник якості AQI, механізми зменшення дублювання шляхом об'єднання однотипних сповіщень у більш інформативні кейси, а також замкнений контур зворотного зв'язку від SOC для адаптивного коригування порогів і параметрів формування алертів [14, 18, 20]. Потік даних формувався на основі журналів автентифікації та доступу, телеметрії кінцевих точок і серверів, мережевих подій захисних засобів і мережевого обладнання, а також журналів критичних сервісів, що дозволило відтворити характерні для підприємства ситуації, у яких алерт є операційною одиницею взаємодії між SIEM і командою реагування.

Для комплексного оцінювання ефективності методики Alert Quality Management експериментальну перевірку проведено за серією типових сценаріїв, які охоплюють як номінальні режими функціонування SIEM/SOC, так і стресові умови перевантаження та зміни контексту експлуатації [8-9]. У номінальних сценаріях S1–S3 моделювалися стандартні режими роботи з помірною інтенсивністю потоку алертів, характерні для повсякденної діяльності підприємства [14]. Зокрема, у сценарії S1 відтворювалася штатна робота систем із поодинокими підозрілими входами, що дозволяло оцінити базові показники ефективності та коректність пріоритезації без впливу надмірного шуму. Сценарії S2 і S3 були орієнтовані на перевірку ризик-орієнтованого скорингу в умовах підбору облікових даних, нетипових спроб доступу та підозрілих змін прав користувачів, коли однакові за формальними ознаками події можуть мати різний пріоритет залежно від критичності активів і ролей суб'єктів доступу.

Стресові сценарії S4–S6 використовувалися для оцінювання стійкості запропонованої методики до alert flood, високої частки хибнопозитивних спрацювань і динамічних змін контексту. У сценарії S4 моделювалося масове надходження однотипних алертів, що дозволяло перевірити ефективність механізмів дедуплікації та зшивання сповіщень у кейси, а також здатність системи стабілізувати чергу SOC [14, 16]. Сценарій S5 відтворював легітимні масові операції, які провокують значну кількість хибнопозитивних алертів, з метою оцінювання впливу зворотного зв'язку SOC і адаптивного тюнінгу порогів на зниження частки FP. У сценарії S6 досліджувалася поведінка системи за умов зміни критичності активів і ролей користувачів, коли ті самі події набувають різного рівня ризику, що дозволяло оцінити адаптивність порогів і уникнення пропуску підтверджених інцидентів [8-9, 18]. Таким чином, сценарії S1–S3 відображають номінальні режими роботи, тоді як S4–S6 — стресові режими перевантаження та зміни контексту, характерні для реальних умов експлуатації SOC.

Параметри експерименту визначалися з урахуванням практики експлуатації SIEM та вимог SLA реагування. Для дедуплікації алертів застосовувалося

часове вікно Δt, у межах якого обчислювалася подібність між алертами за ключовими полями, контекстом і часовою близькістю, а поріг θ_{dup} задавав компроміс між зменшенням дублювання та ризиком об'єднання різних подій. Нормування часових показників обробки виконувалося відповідно до політик SOC за допомогою параметрів θ_{ack} і θ_{close}. Баланс між емпіричною "істинністю" алертів, визначеною за мітками SOC, та контекстним ризиком задавався коефіцієнтом α у формулі корисності $U(a)$. Для адаптивного коригування порогів правил використовувалися параметри η та μ, а також політичні обмеження ρ щодо допустимого рівня хибнопозитивних спрацювань і κ щодо мінімально прийнятної частки підтверджених інцидентів у часовому вікні W [16]. Вагові коефіцієнти ризик-скорингу та показника якості ініціалізувалися експертно та уточнювалися за історичними даними SOC у межах процедури калібрування, спрямованої на мінімізацію сукупних втрат від хибнопозитивних алертів і затримок реагування.

Оцінювання виконувалося за серією типових сценаріїв, які відображають як номінальну роботу, так і умови перевантаження, що є характерними для реальних процесів реагування. У номінальних сценаріях відтворювалися стандартні бізнес-операції та контрольована поява подій, пов'язаних із підбором облікових даних, нетиповими спробами доступу та підозрілими змінами прав, що дозволяло оцінити здатність методики підвищувати пріоритетність критичних алертів без збільшення загального шуму [8-9]. У стресових сценаріях моделювалося лавиноподібне зростання однотипних спрацювань, поява умов, що провокують хибнопозитивні алерти через легітимні масові операції, а також динамічна зміна контексту активів і ролей користувачів, коли однакові за зовнішніми ознаками події можуть мати принципово різні наслідки залежно від критичності ресурсу та привілеїв суб'єкта. Такий набір сценаріїв дозволив оцінити не лише середні показники ефективності, а й стійкість запропонованого підходу до алерт-флуду, високої частки хибнопозитивних спрацювань та змін контексту експлуатації.

Оцінювання виконувалося у режимі порівняння "до/після" для кожного сценарію S1–S6 з подальшою агрегацією результатів. Для кожної метрики (FPR, MTTD, MTTR, навантаження L, середній AQI) обчислювалися середні значення та 95% довірчі інтервали. Для перевірки статистичної значущості відмінностей між режимами застосовувався парний критерій (paired t-test) за умови близької до нормальної розподіленості, або непараметричний тест Манна—Вітні у випадку відхилення від нормальності; рівень значущості приймався $p<0.05$. Такий підхід дозволяє відокремити стабільний ефект методики Alert Quality Management від випадкових коливань, характерних для потоків подій безпеки у стресових режимах.

Результати порівняння режимів "до" і "після" показали, що впровадження методики керування якістю алертів забезпечує одночасне покращення кількох ключових показників ефективності, які безпосередньо відображають операційну спроможність SOC [9]. По-перше, зменшується інтенсивність потоку алертів, оскільки об'єднання однотипних сповіщень знижує дублювання і скорочує кількість повторів, що потрапляють у чергу аналітика, при цьому інформація про розвиток ситуації не втрачається, а навпаки агрегується в більш змістовні кейси [12]. По-друге, зменшується частка хибнопозитивних спрацювань, оскільки структурований зворотний зв'язок від аналітиків використовується як керуючий сигнал для корекції порогів і параметрів правил, завдяки чому процес налаштування переходить від фрагментарного ручного реагування до відтворюваного керування якістю [9]. По-третє, покращуються часові показники реагування, оскільки ризик-орієнтована пріоритезація піднімає у верхню частину черги ті алерти, що мають вищий потенційний вплив з урахуванням критичності активів і контексту користувачів, а зменшення шуму дає можливість швидше приймати рішення щодо справді важливих подій [20]. У підсумку це позитивно впливає на середній час виявлення та обробки, знижує навантаження на аналітиків, підвищує частку виконання цільових показників реагування та формує більш стабільну роботу процесів SOC за рахунок того, що потік алертів стає керованим і вимірюваним.

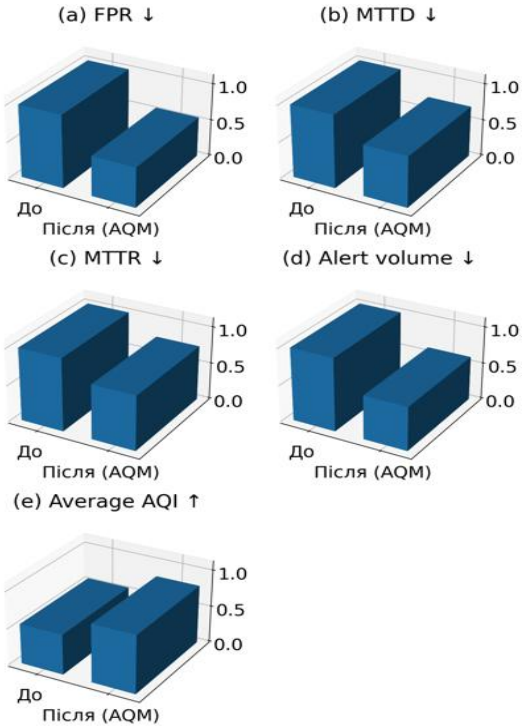

Рис. 6. Порівняння показників "до / після" впровадження Alert Quality Management: (a) FPR, (b) MTTD, (c) MTTR, (d) обсяг алертів, (e) середній $\overline{AQI}$

На рис. 6 подано порівняльну оцінку показників "до / після" впровадження Alert Quality Management (AQM) у вигляді багатопанельного графіка. Підграфік (a) ілюструє зниження частки хибнопозитивних спрацювань (FPR), що свідчить про підвищення точності формування алертів. На підграфіках (b) та (c) показано скорочення середнього часу виявлення (MTTD) і реагування (MTTR), що відображає прискорення роботи SOC за рахунок зменшення шуму та кращої пріоритизації подій. Підграфік (d) демонструє зменшення загального обсягу алертів, що безпосередньо знижує операційне навантаження на аналітиків. Натомість підграфік (e) показує зростання середнього індексу якості алертів $\overline{AQI}$, підтверджуючи, що впровадження AQM не лише зменшує кількість алертів, а й підвищує їхню інформативність і керованість у процесах SOC.

Узагальнюючи отримані результати, можна зробити висновок, що підвищення експлуатаційної ефективності SIEM досягається не стільки шляхом нарощування складності детекційних правил чи моделей, скільки через системне керування якістю алертів як операційного ресурсу: зменшення дублювання, зниження частки хибнопозитивних спрацювань, контекстну пріоритезацію за ризиком та організацію замкненого контуру зворотного зв'язку, який перетворює рішення аналітиків на формальні керуючі дії для налаштування SIEM.

На рис. 7 проілюстровано динамічну реакцію системи на стрес-сценарій різкого зростання кількості алертів.

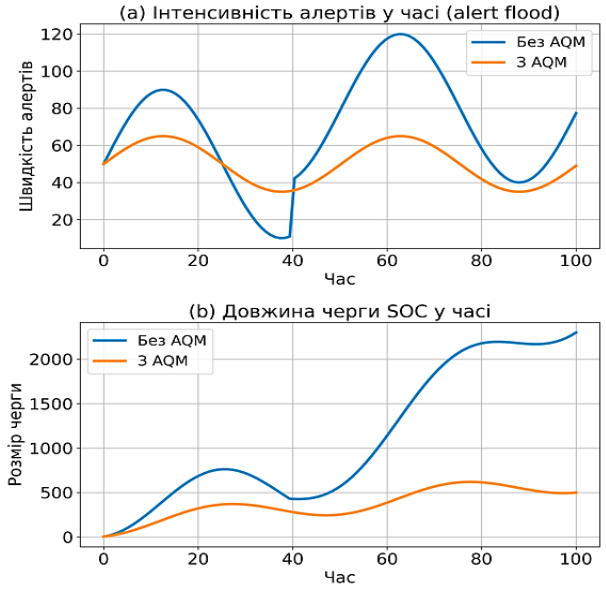

Рис. 7. Поведінка SIEM/SOC у стрес-сценаріях масового надходження алертів (alert flood)

Підграфік (a) відображає інтенсивність надходження алертів у часі: у режимі *без AQM* спостерігаються значні коливання та пікові навантаження, тоді як застосування Alert Quality Management (AQM) забезпечує згладжування потоку алертів. Підграфік (b) демонструє зміну довжини черги SOC: за відсутності AQM черга швидко зростає, що призводить до втрати керованості процесу реагування, тоді як у режимі *з AQM* її розмір стабілізується [9, 12, 18]. Отримані результати підтверджують, що запропонована методика підвищує стійкість SIEM/SOC не лише за середніми показниками, а й у критичних умовах перевантаження.

Саме така логіка дозволяє забезпечити вимірюваний ефект у ключових показниках, що характеризують здатність підприємства своєчасно виявляти та обробляти інциденти, не допускаючи перевантаження команди реагування та деградації якості моніторингу в умовах зростання обсягів подій і складності загроз.

Висновки. У статті розв'язано науково-прикладну проблему підвищення експлуатаційної ефективності SIEM шляхом переходу від локального «ручного» тюнінгу правил до системного керування якістю алертів як керованого операційного об'єкта в процесах SOC. Запропонована методика Alert Quality Management формалізує життєвий цикл алерта, поєднує ризик-орієнтований скоринг з урахуванням контексту (критичність активу, роль користувача, загрозове середовище), інтегральний показник якості AQI та механізми дедуплікації/зшивання алертів у кейси. Ключовим елементом наукової новизни є замкнений контур зворотного зв'язку SOC, у якому мітки TP/FP/BENIGN/TUNE агрегуються за правилами та використовуються як керуючий сигнал для адаптивного оновлення порогів і параметрів формування алертів у часі.

Експериментальні результати підтверджують практичну цінність підходу: у порівнянні режимів «до/після» впровадження AQM зафіксовано узгоджене покращення ключових KPI (зниження FPR, скорочення MTTD і MTTR, зменшення обсягу алертів при одночасному зростанні середнього AQI), що прямо відображає зменшення операційного навантаження на SOC і підвищення керованості потоку сповіщень. Додатково продемонстровано стійкість методики у стрес-сценаріях alert flood: застосування AQM забезпечує згладжування потоку алертів і стабілізацію черги SOC, тоді як без AQM спостерігається неконтрольоване накопичення черги та деградація керованості реагування. Отже, підвищення ефективності SIEM досягається не стільки ускладненням детекційних моделей, скільки керованим використанням контексту, дедуплікації та формалізованого зворотного зв'язку SOC, що робить оптимізацію якості алертів відтворюваною, вимірюваною та придатною для практичного впровадження в підприємстві.

Список літератури

[1] Tariq, S., Baruwal Chhetri, M., Nepal, S., & Paris, C. (2025). Alert fatigue in security operations centres:

Research challenges and opportunities. *ACM Computing Surveys, 57*, Article 224. https://doi.org/10.1145/3723158

[2] Jalalvand, F., Baruwal Chhetri, M., Nepal, S., & Paris, C. (2024). Alert prioritisation in security operations centres: A systematic survey on criteria and methods. *ACM Computing Surveys, 57*. https://doi.org/10.1145/3695462

[3] Landauer, M., Skopik, F., Wurzenberger, M., & Rauber, A. (2022). Dealing with security alert flooding: Using machine learning for domain-independent alert aggregation. *ACM Transactions on Privacy and Security, 25*. https://doi.org/10.1145/3510581

[4] Oliver, J., Batta, R., Bates, A., Inam, M. A., Mehta, S., & Xia, S. (2024). *Carbon filter: Real-time alert triage using large scale clustering and fast search* (arXiv:2405.04691). arXiv. https://arxiv.org/abs/2405.04691

[5] Turcotte, M., Labrèche, F., & Paquette, S. O. (2025). *Automated alert classification and triage (AACT): An intelligent system for the prioritisation of cybersecurity alerts* (arXiv:2505.09843). arXiv. https://arxiv.org/abs/2505.09843

[6] Macaneata, C. (2024). Overview of security information and event management systems. *Informatica Economica, 28*(1), 15–24.

[7] Tendikov, N., Rzayeva, L., Saoud, B., Shayea, I., Bin Azmi, M., Myrzatay, A., & Alnakhli, M. (2024). Security information event management data acquisition and analysis methods with machine learning principles. *Results in Engineering, 22*, 102254. https://doi.org/10.1016/j.rineng.2024.102254

[8] Lund, B. D., Lee, T.-H., Wang, Z., Wang, T., & Mannuru, N. R. (2024). Zero trust cybersecurity: Procedures and considerations in context. *Encyclopedia, 4*(4), 1520–1533. https://doi.org/10.3390/encyclopedia4040096

[9] Wang, X., Yang, X., Liang, X., Zhang, X., Zhang, W., & Gong, X. (2023). Combating alert fatigue with AlertPro: Context-aware alert prioritization using reinforcement learning for multi-step attack detection. *Computers & Security, 137*, Article 103583. https://doi.org/10.1016/j.cose.2023.103583

[10] Rzaeva, S., Skladannyi, P., Kostiuk, Y., Abramov, V., & Kravchenko, V. (2025). Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security, 31*(1), 23–36. https://doi.org/10.18372/2225-5036.31.20634

[11] Ojo, C., Bassey, C., & Idowu, S. (2024). Alert prioritization techniques in security monitoring: A focus on severity averaging and alert entities. *Saudi Journal of Engineering and Technology, 9*, 334–339. https://doi.org/10.36348/sjet.2024.v09i07.008

[12] Довженко, Н., Іваніченко, Є., & Костюк, Ю. (2025). Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими IOT-компонентами на основі графових моделей. *Кібербезпека: освіта, наука, техніка, 1*(29), 762–776. https://doi.org/10.28925/2663-4023.2025.29.938

[13] Jiang, Y., Meng, Q., Shang, F., Oo, N., Minh, L., Lim, H., & Sikdar, B. (2025). *MITRE ATT&CK applications in cybersecurity and the way forward* (arXiv:2502.10825). arXiv. https://doi.org/10.48550/arXiv.2502.10825

[14] Костюк, Ю., Складанний, П., Рзаєва, С., Мазур, Н., Черевик, В., & Аносов, А. (2025). Особливості реалізації мережевих атак через TCP/IP-протоколи. *Кібербезпека: освіта, наука, техніка, 1*(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915

[15] González-Granadillo, G., González-Zarzosa, S., & Díaz, R. (2021). Security information and event management (SIEM): Analysis, trends and usage in critical infrastructures. *Sensors, 21*(14), Article 4759. https://doi.org/10.3390/s21144759

[16] Складанний, П., Костюк, Ю., Рзаєва, С., Самойленко, Ю., & Савченко, Т. (2025). Розробка модульних нейронних мереж для виявлення різних класів мережевих атак. *Кібербезпека: освіта, наука, техніка, 3*(27), 534–548. https://doi.org/10.28925/2663-4023.2025.27.772

[17] Thapliyal, V., & Thapliyal, P. (2024). Machine learning for cybersecurity: Threat detection, prevention, and response. *Darpan International Research Analysis, 12*, 1–7. https://doi.org/10.36676/dira.v12.i1.01

[18] Костюк, Ю., Складанний, П., Рзаєва, С., Самойленко, Ю., & Коршун, Н. (2025). Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. *Кібербезпека: освіта, наука, техніка, 2*(30), 125–156. https://doi.org/10.28925/2663-4023.2025.30.956

[19] Singh, A., & III, R. (2025). Contextual threat intelligence and alert prioritization with Foundation-Sec-8b. *International Journal of Artificial Intelligence Research and Development, 3*, 131–145. https://doi.org/10.34218/IJAIRD_03_01_009

[20] Костюк, Ю., Хорольська, К., Бебешко, Б., Довженко, Н., Коршун, Н., & Пазинін, А. (2025). Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. *Кібербезпека: освіта, наука, техніка, 4*(28), 633–655. https://orcid.org/0009-0002-9506-9539

[21]. Behl, A., Bapna, R., Gupta, A., & Telang, R. (2023). Cybersecurity incident response: Evidence from security operations centers. *Information Systems Research, 34*(2), 712–734. https://doi.org/10.1287/isre.2022.1149

[22]. Sommer, R., & Paxson, V. (2024). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Security & Privacy, 22*(1), 64–72. https://doi.org/10.1109/MSEC.2023.3322897

[23]. Ganesan, R., Shah, A., Jajodia, S., & Cam, H. (2019). *Optimizing alert data management processes at a cyber ecurity operations center*. In S. Jajodia, G. Cybenko, P. Liu, C. Wang, & M. Wellman (Eds.), Adversarial and Uncertain Reasoning for Adaptive Cyber Defense (pp. 206–231). Springer. https://doi.org/10.1007/978-3-030-30719-6_9

[24]. Kosle, A. R. (2025). *Reducing alert fatigue in SOC teams through contextual prioritization and threat intelligence integration* (OSF Preprint). Open Science Framework. https://doi.org/10.31219/osf.io/a2qd5_v1

УДК 004.056

Kostiuk Y., Skladannyi P., Rzaeva S. Alert quality management in SIEM based on risk-oriented scoring and SOC feedback (alert quality management)

Abstract. *This paper proposes a methodology for managing alert quality in Security Information and Event Management (SIEM) systems based on risk-oriented scoring and a closed-loop feedback mechanism from the Security Operations Centre (SOC). The relevance of the study is driven by the overload of SOC analysts caused by excessive numbers of alerts, a large share of which have low analytical value and do not result in confirmed security incidents. Unlike approaches that primarily focus on improving event correlation or increasing detection accuracy, the proposed methodology treats an alert as a controllable operational object and formalizes its quality using an integral indicator, the Alert Quality Index (AQI). This indicator accounts for the alert's usefulness for response, the time relevance of its processing, the level of alert duplication, and the consumption of SOC analytical resources. Alert risk scoring is adjusted by asset criticality, user roles, and the threat context, thereby aligning SIEM technical signals with the potential impact of incidents on the enterprise's business processes. To mitigate alert flooding, deduplication mechanisms and alert stitching are applied to consolidate similar notifications into more informative cases using a similarity metric within a specified time window. SOC analyst decisions (TP, FP, BENIGN, TUNE) are used as a control signal for adaptive tuning of thresholds and parameters of SIEM rules. Experimental evaluation across a series of nominal and stress scenarios demonstrated a reduction in the false positive rate, shorter MTTD and MTTR, decreased SOC workload, and an increase in the average AQI, confirming the effectiveness of systematic alert flow management under real operational conditions.*

Keywords: *SIEM, SOC, alert fatigue, alert quality management, risk-oriented scoring, security incidents, deduplication, feedback.*

Костюк Юлія Володимирівна, PhD, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Yuliia Kostiuk, PhD, Associate Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok Borys Grinchenko Kyiv Metropolitan University.

Складанний Павло Миколайович, кандидат технічних наук, доцент, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Pavlo Skladannyi, PhD, Associate Professor, Head of the Department of Information and Cyber Security named after Professor Volodymyr Buryachok Borys Grinchenko Kyiv Metropolitan University.

Рзаєва Світлана Леонідівна, кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук Київського столичного університету імені Бориса Грінченка.
Rzaeva Svitlana, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Science Borys Grinchenko Kyiv Metropolitan University.