30. Asfha A. E., Vaish A. Information Security Risk Assessment in Industry Information System Based on Fuzzy Set Theory and Artificial Neural Network // Informatics and Automation. 2024. Т. 23, № 2. P. 542–571. DOI: https://doi.org/10.15622/ia.23.2.9.

31.National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1) [Електронний ресурс]. Gaithersburg, MD: National Institute of Standards and Technology, 2023. DOI: https://doi.org/10.6028/NIST.AI.100-1.

Надійшла до редакції (Received): 10.02.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

http://creativecommons.org/licenses/by/4.0/
This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.

УДК 004.056.55:004.7.056
DOI: 10.31673/2409-7292.2026.011393

Костюк Ю.В., Складанний П.М.

КРИПТОГРАФІЧНА МОДЕЛЬ ДОВІРИ ДО ПОДІЙ БЕЗПЕКИ В SIEM ДЛЯ ІНТЕЛЕКТУАЛЬНОГО ФОРМУВАННЯ МЕРЕЖЕВИХ ІНЦИДЕНТІВ

У статті запропоновано підхід до інтелектуального формування мережевих інцидентів у системах управління подіями та інцидентами інформаційної безпеки (SIEM), що ґрунтується на криптографічній моделі довіри до подій безпеки. Актуальність дослідження зумовлена інтенсивною цифровізацією корпоративних комп'ютерних мереж, зростанням обсягів телеметрії, широким використанням хмарних сервісів і розподілених інфраструктур, у яких традиційні механізми кореляції подій дедалі частіше виявляються вразливими до маніпуляцій вхідними даними. У більшості сучасних SIEM-рішень події безпеки розглядаються як апріорно достовірні за умови їх надходження з легітимних журналів або сенсорів, що є ризикованим у середовищах зі змінним рівнем довіри. За таких умов події можуть бути згенеровані скомпрометованими вузлами, змінені під час передавання чи зберігання або навмисно ін'єктовані зловмисником з метою спотворення процесу кореляції. Метою роботи є розроблення та наукове обґрунтування моделі, у межах якої кожна подія безпеки інтерпретується як криптографічно оформлене твердження про стан комп'ютерної мережі, придатне до формальної перевірки та кількісного оцінювання достовірності. Запропоновано перенести довіру з рівня джерел телеметрії на рівень окремих подій із використанням криптографічних механізмів фіксації походження, цілісності, контексту генерації та часової прив'язки. На цій основі формується пояснювана оцінка довіри до події, яка інтегрується в механізми кореляції та використовується як ваговий чинник під час формування інцидентів.У статті розглянуто алгоритмічні засади потокової обробки подій, що поєднують криптографічну верифікацію, оцінювання довіри та зважену кореляцію в межах кореляційних вікон, забезпечуючи масштабованість для високонавантажених середовищ. Практичне значення отриманих результатів полягає у можливості інтеграції запропонованої моделі в існуючі SIEM-архітектури без зміни принципів збору телеметрії, зі зменшенням кількості хибних спрацьовувань, підвищенням стійкості до ін'єкції та підміни подій і покращенням якості сформованих мережевих інцидентів для подальшого реагування та роботи SOC.

Ключові слова: SIEM, події безпеки, криптографічна верифікація, модель довіри, кореляція подій, мережеві інциденти, ін'єкція, підміна подій.

Вступ

Інтенсивна цифровізація корпоративних комп'ютерних мереж, широке використання хмарних сервісів і розподілених інфраструктур зумовлюють стрімке зростання кількості подій безпеки, що підлягають аналізу в системах управління подіями та інцидентами інформаційної безпеки (SIEM) [1, 5, 7, 9]. За таких умов ефективність захисту мережі дедалі більше залежить не від , можливостей збору телеметрії, а від здатності SIEM-систем коректно інтерпретувати події, відрізняти дійсні загрози від шуму та формувати обґрунтовані інциденти безпеки.

Попри значний розвиток методів кореляції подій, сучасні SIEM-рішення переважно ґрунтуються на припущенні про апріорну достовірність подій безпеки, отриманих із журналів,

© Прокопович-Ткаченко Д.І., Єжихін А.В., Бушков В.Г., Черкаський О.В., Черкаський Д.О. Формування цільового цифрового профілю безпеки мереж електронних комунікацій в умовах гібридних кібератак: ризик-орієнтований та багатокритеріальний підхід. Сучасний захист інформації, 1(65), 87–103. https://doi.org/10.31673/2409-7292.2026.011184

мережевих сенсорів або агентів кінцевих точок [1-3, 6, 11]. Такий підхід є вразливим у середовищах з низьким або змінним рівнем довіри, де події можуть бути згенеровані компрометованими вузлами, модифіковані в процесі передавання або навмисно ін'єктовані зловмисником з метою маніпуляції механізмами кореляції. У результаті SIEM оперує подіями як фактами, не маючи формальних засобів перевірки їх цілісності, походження та контекстної узгодженості.

Особливої актуальності ця проблема набуває в комп'ютерних мережах із високим рівнем автоматизації реагування, де результати кореляції подій безпосередньо впливають на політики доступу, ізоляцію вузлів або запуск захисних сценаріїв [6, 9-11]. За відсутності формалізованої моделі довіри до подій помилкові або підроблені повідомлення можуть призводити до хибних інцидентів, необґрунтованих дій реагування та зниження загальної стійкості мережі.

У дослідженні запропоновано новий підхід до формування мережевих інцидентів у SIEM, що базується на криптографічній моделі довіри до подій безпеки. На відміну від традиційних рішень, у межах запропонованої концепції подія безпеки розглядається як криптографічно оформлене твердження про стан мережі, достовірність якого може бути формально перевірена та кількісно оцінена [2-4]. Довіра переноситься з рівня джерела або каналу збору телеметрії на рівень окремої події, що дозволяє будувати кореляційні механізми, стійкі до підробки, повторного відтворення та контекстних маніпуляцій.

Наукова новизна роботи полягає у введенні нового об'єкта аналізу в SIEM – рівня довіри до події безпеки, який формується з використанням криптографічних механізмів фіксації походження, цілісності та контексту генерації подій [2-3, 6, 14, 20]. Запропоновано принципово новий підхід до формування інцидентів, у якому кореляція подій виконується не лише за часовими або семантичними ознаками, а з урахуванням їх криптографічної достовірності та ризикової значущості для мережі.

Теоретичне значення отриманих результатів полягає в розвитку концептуальних засад SIEM як інтелектуальної системи, здатної оперувати формалізованими твердженнями про безпеку мережі [13, 17-18]. Запропонована криптографічна модель довіри до подій розширює існуючі підходи до аналізу подій безпеки, створюючи підґрунтя для подальших досліджень у напрямі формального моделювання довіри, верифікованої кореляції та побудови пояснюваних механізмів прийняття рішень у системах кіберзахисту.

Практичне значення дослідження полягає у можливості застосування запропонованої моделі в реальних SIEM-системах для підвищення якості формування мережевих інцидентів, зменшення кількості хибних спрацьовувань і підвищення стійкості до атак, спрямованих на підміну або ін'єкцію подій [9-11]. Запропонований підхід може бути інтегрований у існуючі архітектури SIEM без зміни принципів збору телеметрії, що робить його придатним для практичного впровадження в корпоративних комп'ютерних мережах.

Метою дослідження є розроблення та наукове обґрунтування криптографічної моделі довіри до подій безпеки в системах SIEM, яка забезпечує інтелектуальне формування мережевих інцидентів на основі криптографічно перевірюваних властивостей подій з урахуванням їх походження, цілісності, контексту генерації та ризикової значущості для комп'ютерної мережі [6, 14]. Досягнення поставленої мети передбачає подолання обмежень традиційних підходів до кореляції подій, у яких події безпеки розглядаються як апріорно достовірні, без формалізованого механізму оцінювання рівня довіри до них.

Для реалізації зазначеної мети в роботі здійснюється аналіз сучасних підходів до формування інцидентів у SIEM з погляду забезпечення достовірності подій у комп'ютерних мережах, що дозволяє виявити ключові обмеження існуючих рішень у частині вразливості до підробки, повторного відтворення та контекстних маніпуляцій подіями [5-6, 11, 16]. На цій основі формується формалізоване подання події безпеки як криптографічно оформленого твердження про стан мережі, що включає не лише семантичний опис, а й контекст генерації, часові характеристики та механізми забезпечення цілісності й автентичності.

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

Подальше дослідження зосереджується на розробленні криптографічної моделі формування рівня довіри до подій безпеки, яка ґрунтується на верифікації їх походження, цілісності та узгодженості з мережевим контекстом функціонування [14, 17-18, 20]. Отриманий рівень довіри використовується як кількісна характеристика, що інтегрується в процес кореляції подій та дозволяє перейти від синтаксичного об'єднання подій до інтелектуального формування мережевих інцидентів з урахуванням їх фактичної достовірності та потенційного впливу на безпеку мережі.

Завершальним етапом дослідження є розроблення алгоритмічних засад агрегації та зважування подій безпеки в SIEM на основі криптографічної довіри та ризикової значущості, а також оцінювання ефективності запропонованого підходу з погляду якості формування інцидентів, зменшення кількості хибних спрацьовувань і підвищення стійкості SIEM до цілеспрямованих маніпуляцій подіями в комп'ютерних мережах.

Аналіз літературних джерел і постановка проблеми

Проблематика управління подіями та інцидентами інформаційної безпеки в корпоративних комп'ютерних мережах активно досліджується у сучасних наукових роботах, що зумовлено зростанням обсягів мережевої телеметрії, ускладненням атак і підвищенням вимог до оперативності реагування. У ґрунтовному дослідженні González-Granadillo, González-Zarzosa та Diaz [1] наведено систематичний аналіз еволюції SIEM-систем, визначено їх роль у критичних інфраструктурах та окреслено ключові напрями розвитку, серед яких особливу увагу приділено кореляції подій і автоматизації аналізу. Водночас автори підкреслюють, що ефективність SIEM значною мірою обмежується якістю подій, які надходять до системи, та відсутністю механізмів оцінювання їх достовірності.

Окремий напрям досліджень пов'язаний із забезпеченням цілісності та захисту журналів подій. У роботі Soriano-Salvador та Guardiola-Múzquiz [2] запропоновано файлову систему SealFS, яка реалізує механізми tamper-evident logging на основі криптографічних примітивів. Подальший розвиток цього підходу представлено в роботі Guardiola-Múzquiz та Soriano-Salvador [3], де запропоновано комбінацію зберігання та криптографічного «ratcheting» для підвищення стійкості журналів до підробки. Попри високий рівень захисту логів, зазначені підходи орієнтовані переважно на післяфактну верифікацію цілісності та не інтегруються безпосередньо в процес кореляції подій або формування інцидентів у SIEM.

У роботі Reijsbergen, Maw, Yang, Dinh та Zhou [4] розглянуто концепцію прозорих і приватних сервісів обробки даних, що забезпечують перевірюваність і контроль доступу до інформації в розподілених середовищах. Запропоновані механізми створюють передумови для формування довіри до даних, однак не враховують специфіку подій інформаційної безпеки та не адаптовані до задач кореляції мережевих подій у SIEM.

Сучасні дослідження також активно використовують методи машинного навчання для аналізу подій безпеки. У роботі Tendikov, Rzayeva, Saoud, Shayea, Bin Azmi, Myrzatay та Alnakhli [5] запропоновано підходи до збору й аналізу даних SIEM із використанням алгоритмів машинного навчання, що дозволяє підвищити ефективність виявлення загроз. Водночас у цьому підході події аналізуються з позицій статистичних і поведінкових ознак без урахування криптографічної перевірюваності їх походження та цілісності. Аналогічні обмеження характерні для ієрархічної моделі кореляції подій, запропонованої Maosa, Ouazzane та Ghanem [6], у якій основна увага приділяється структурі кореляційних правил і часовій узгодженості подій.

Питання вдосконалення архітектури та відповідності SIEM сучасним вимогам розглядаються у роботі Velásquez, Monterrubio, Crespo та співавт. [7], де запропоновано концепцію сталого та нормативно відповідного SIEM. Проте навіть у межах цього підходу події безпеки розглядаються як апріорно достовірні, без формалізованої моделі довіри до них.

Значна кількість досліджень присвячена оптимізації правил виявлення атак і зменшенню навантаження на аналітиків SOC. Зокрема, Uccello, Pawlicki, D'Antonio, Kozik та Choraś [8]

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

демонструють ефективність rule-based підходів до виявлення DoS-атак, тоді як Jalalvand, Baruwal Chhetri, Nepal та Paris [9] виконують систематичний огляд методів пріоритизації алертів у SOC. Проблема перевантаження аналітиків та явище alert fatigue детально досліджуються у роботі Tariq, Baruwal Chhetri, Nepal та Paris [10]. Разом із тим, у всіх зазначених підходах події безпеки розглядаються як рівнозначні одиниці аналізу, незалежно від рівня довіри до їх походження або цілісності.

Проведений аналіз літературних джерел свідчить, що, попри активний розвиток SIEM-технологій, криптографічні механізми використовуються переважно для захисту журналів або даних зберігання, але не інтегруються безпосередньо в логіку формування мережевих інцидентів [1-3, 6, 14, 16, 20, 22]. Відсутність формалізованої криптографічної моделі довіри до подій безпеки обмежує можливості інтелектуальної кореляції та створює передумови для маніпуляцій подіями в комп'ютерних мережах, що зумовлює необхідність подальших досліджень у цьому напрямі.

Виклад основного матеріалу

У сучасних системах управління подіями та інцидентами інформаційної безпеки довіра традиційно асоціюється з джерелами даних, сенсорами або мережевими вузлами, з яких надходить телеметрія [1, 22]. Передбачається, що події, згенеровані легітимним джерелом або перевіреним агентом, є апріорно достовірними та можуть без додаткової перевірки використовуватися в механізмах кореляції. Такий підхід був виправданим у відносно статичних мережах із чітко визначеними доменами довіри, однак у сучасних розподілених і динамічних комп'ютерних мережах він дедалі частіше призводить до помилкових інтерпретацій стану безпеки.

Ключовою проблемою є те, що навіть за формально довіреного джерела або сенсора окремі події безпеки можуть бути скомпрометовані на етапах генерації, передавання чи зберігання, а також унаслідок навмисної ін'єкції подій зловмисником [11, 22]. За таких умов довіра до джерела не гарантує достовірності кожної події, що зумовлює необхідність перегляду традиційної моделі довіри в SIEM.

У роботі розглядається клас атак, спрямованих на маніпуляцію телеметрією SIEM, зокрема ін'єкція подій, підміна та модифікація у каналах передавання, повторне відтворення валідних подій поза первинним контекстом, контекстна підміна та кореляційні приманки [14, 16]. Такі впливи є критичними, оскільки спотворюють вхідні факти та знижують якість інцидентів незалежно від потужності кореляційного ядра [6, 18, 20]. Існуючі моделі довіри до джерел, сенсорів, користувачів або вузлів не враховують їх змінний стан у часі та можливість часткової компрометації, що унеможливлює відокремлення коректних подій від навмисно підроблених.

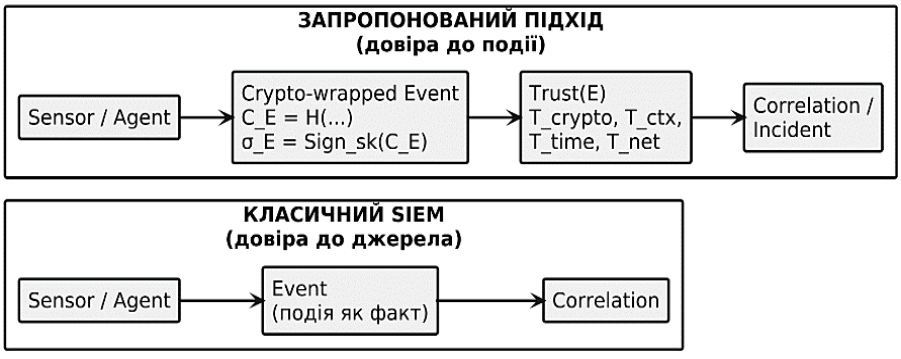

Рис. 1. Концептуальне порівняння підходів до формування довіри в SIEM: довіра до джерела та довіра до події

Це зумовлює перехід від довіри до джерел до довіри на рівні окремої події, яка розглядається як твердження про стан мережі в певний момент часу та може бути

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

формалізована з погляду істинності, достовірності й довіри [4, 14]. Як показано на рис. 1, у традиційних SIEM-системах події безпеки використовуються в механізмах кореляції без явної формалізації їх достовірності, тоді як у запропонованому підході подія розглядається як криптографічно верифіковане твердження, для якого рівень довіри кількісно оцінюється до етапу кореляції.

Розгляд події як твердження дозволяє застосовувати до неї криптографічні механізми фіксації походження, цілісності та контексту генерації, надаючи події активних перевірюваних властивостей, незалежних від джерела [2-4, 6, 20]. Це створює підґрунтя для кількісного оцінювання рівня довіри до події та використання цієї оцінки як одного з ключових факторів формування мережевих інцидентів.

У такій постановці задача довіри до подій у SIEM зводиться до визначення достовірності окремих тверджень про стан мережі з урахуванням їх криптографічних властивостей, контексту та узгодженості з іншими подіями, що інтегрує рівень довіри безпосередньо в логіку прийняття рішень SIEM [6-7, 20]. Запропонований підхід створює основу для формалізації криптографічної моделі події та розроблення алгоритмів інтелектуального формування інцидентів з урахуванням рівня довіри до їх фактичної достовірності.

Формалізація події безпеки як криптографічно оформленого твердження

Для реалізації концепції довіри до подій безпеки необхідно перейти від неформального трактування події як запису журналу до її строгого формального подання [2-4, 20]. У межах запропонованого підходу подія безпеки розглядається як структуроване твердження про стан комп'ютерної мережі в певний момент часу, яке може бути об'єктом криптографічної верифікації та кількісного оцінювання достовірності [6]. Подію безпеки формально визначимо у вигляді впорядкованого кортежу:

$$E = \langle id, src, t, ctx, payload \rangle, \tag{1}$$

де id – унікальний ідентифікатор події, src – джерело генерації події (мережевий вузол, сенсор, агент або сервіс), t – часовий параметр, що фіксує момент виникнення події, ctx – контекст генерації, який описує мережеві, системні та середовищні умови, за яких була сформована подія, $payload$ – семантичне навантаження події, що містить інформацію про виявлену активність або зміну стану мережі [14, 16, 20]. Таке подання дозволяє інтерпретувати подію не як ізольований лог-запис, а як формалізоване твердження виду «в системі з джерела src у момент часу t за контексту ctx відбулася подія зі змістом $payload$». Важливою особливістю є явне виділення контексту ctx, який відіграє ключову роль у подальшому оцінюванні достовірності події та її узгодженості з іншими подіями в системі.

Для забезпечення можливості перевірки цілісності та незмінності події вводиться криптографічне зобов'язання (commitment), яке зв'язує між собою основні компоненти події. Криптографічне зобов'язання для події E визначається як:

$$C_E = H(E \| ctx \| t), \tag{2}$$

де $H(\cdot)$ – криптографічна хеш-функція, а оператор $\|$\parallel$\|$ позначає конкатенацію. Таке зобов'язання фіксує не лише семантичний вміст події, але й її контекст та часову прив'язку, унеможливлюючи їх непомітну зміну без порушення хеш-значення.

У разі підвищених вимог до автентичності події криптографічне зобов'язання може бути доповнене або замінене цифровим підписом:

$$\sigma_E = Sign_{sk}(C_E), \tag{3}$$

де $Sign_{sk}(\cdot)$ – алгоритм цифрового підпису з використанням секретного ключа джерела події. У такому випадку подія набуває властивості криптографічно підтвердженого твердження, походження якого може бути перевірене незалежно від каналу передавання або системи зберігання.

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

На рис. 2 показано структуру події безпеки як криптографічно оформленого твердження та процедуру верифікації ($C_E,\ \sigma_E$), яка забезпечує перевірку цілісності й автентичності походження події перед її подальшою обробкою в SIEM.

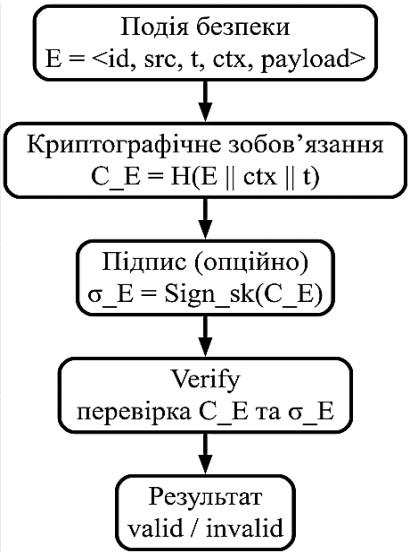

Рис. 2. Криптографічне оформлення та верифікація події безпеки

Запропоноване криптографічне оформлення події забезпечує набір властивостей, які безпосередньо використовуються далі в моделі довіри та формуванні інцидентів [6, 20]. По-перше, гарантується цілісність події: будь-яка зміна компонентів $\langle id, src, t, ctx, payload\rangle$ неминуче призводить до невідповідності криптографічного зобов'язання C_E, що унеможливлює непомітну модифікацію змісту події. По-друге, реалізується зв'язування з контекстом і часом, оскільки подія не може бути коректно "перенесена" в інший ctx або інший момент часу t без порушення зобов'язання, тобто без втрати криптографічної узгодженості. По-третє, за наявності цифрового підпису σ_E забезпечується автентичність походження: валідність події може бути перевірена незалежно від транспортного каналу та сховища, що зменшує залежність SIEM від апріорної довіри до інфраструктури доставки й зберігання телеметрії [2, 22]. Нарешті, досягається стійкість до replay у зміненому середовищі: повторне відтворення події поза первинним контекстом призводить до зниження $T_{ctx}(E)$ і/або $T_{time}(E)$, що обмежує її вплив на формування інциденту навіть у випадку коректного підпису [14, 16, 20]. Таким чином, криптографічні примітиви в запропонованій моделі виступають не просто "захистом логів", а вхідними доказовими ознаками, які безпосередньо керують механізмами кореляції через величину $Trust(E)$.

Запропоноване криптографічне оформлення події принципово відрізняється від традиційних підходів до захисту журналів, у яких криптографічні механізми застосовуються переважно для післяфактної перевірки цілісності або аудиту [22]. У межах запропонованої моделі криптографічне зобов'язання виступає активним елементом аналізу, що безпосередньо впливає на подальшу обробку події в SIEM.

Хеш або цифровий підпис забезпечує криптографічний зв'язок між подією, її контекстом і часом виникнення, унеможливлюючи повторне відтворення, підміну часових характеристик і ін'єкцію подій у невідповідному середовищі. У результаті подія стає самодостатнім об'єктом довіри, властивості якого можуть бути перевірені незалежно від апріорної надійності джерела. Таким чином, криптографічне оформлення події створює основу для кількісного оцінювання довіри та її використання в інтелектуальних механізмах формування інцидентів, перетворюючи подію з пасивного запису журналу на активне криптографічно верифіковане твердження про стан мережі.

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

Криптографічна модель формування рівня довіри до події безпеки

Запропонована криптографічна модель довіри до подій безпеки ґрунтується на ідеї кількісного оцінювання достовірності окремого твердження про стан комп'ютерної мережі. На відміну від традиційних підходів, у яких події розглядаються як рівнозначні елементи кореляції, у межах цієї моделі кожна подія характеризується власним рівнем довіри, що визначається сукупністю формально перевірюваних ознак [14]. Рівень довіри до події безпеки E визначається як скалярна величина:

$$Trust(E) \in [0,1], \tag{4}$$

де значення, близькі до 1, відповідають високій достовірності події, а значення, близькі до 0, – подіям із низьким рівнем довіри або потенційно скомпрометованим твердженням [20]. Значення $Trust(E) = 0$ відповідає подіям, що не пройшли базову криптографічну верифікацію та не можуть бути використані в процесі формування інцидентів.

Першою та необхідною складовою рівня довіри є результат криптографічної верифікації події, який відображає цілісність і автентичність її вмісту. Нехай C_E – криптографічне зобов'язання події, визначене в попередньому розділі, σ_E – цифровий підпис (за наявності). Тоді показник криптографічної верифікації визначається як:

$$T_{crypto}(E) = \begin{cases} 1, & \text{якщо } C_E \text{ коректний і } \sigma_E \text{ валідний,} \\ 0, & \text{в іншому випадку} \end{cases}. \tag{5}$$

У разі використання лише хеш-зобов'язання без підпису $T_{crypto}(E)$ може приймати проміжні значення, що відображають ступінь упевненості у незмінності події з урахуванням довіри до каналу передавання або середовища зберігання.

Другою складовою є оцінювання узгодженості контексту ctx події з поточним або очікуваним станом комп'ютерної мережі. Контекст включає параметри мережевого середовища, ролі вузлів, активні з'єднання та системні стани. Узгодженість контексту визначається функцією:

$$T_{ctx}(E) = 1 - \delta(ctx_E, ctx_{ref}), \tag{6}$$

де $\delta(\cdot)$ – нормалізована міра відхилення контексту події від референтного або очікуваного контексту ctx_{ref}. Значення $T_{ctx}(E)$ наближається до 1 за умови повної узгодженості контексту та зменшується зі зростанням аномальних або нетипових параметрів. Функція $\delta(\cdot)$ може реалізовуватися як статистична або нейромережева міра відхилення [15], що виявляє приховані аномальні структури в багатовимірному контексті події (ctx) на основі спостережуваної телеметрії.

Часова складова рівня довіри відображає актуальність події та її узгодженість із часовою динамікою інших подій [14, 16]. Події, що мають значну часову затримку або порушують причинно-часову послідовність, вважаються менш достовірними. Часовий показник визначається як:

$$T_{time}(E) = e^{-\lambda|t_E - t_{ref}|}, \tag{7}$$

де t_E – час генерації події, t_{ref} – референтний часовий момент або інтервал, λ – параметр чутливості до часових відхилень.

Мережеві ознаки відображають відповідність події поточній топології, політикам маршрутизації та очікуваним потокам трафіку [22]. До таких ознак належать джерело та призначення трафіку, тип протоколу, напрямок з'єднання та роль вузла в мережі. Мережевий показник довіри визначається функцією:

$$T_{net}(E) \in [0,1], \tag{8}$$

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

яка зменшується у разі виявлення суперечностей між подією та відомою мережею конфігурацією або політиками безпеки. Оцінювання $T_{net}(E)$ може спиратися на статистичні та нейромережеві методи аналізу мережевих профілів [15], які виділяють нетипові поєднання параметрів трафіку та приховані аномальні закономірності.

Загальний рівень довіри до події формується шляхом агрегування окремих складових із використанням зваженої адитивної моделі [20]:

$$Trust(E) = w_1 T_{crypto}(E) + w_2 T_{ctx}(E) + w_3 T_{time}(E) + w_4 T_{net}(E), \quad (9)$$

де $w_i \geq 0$, $\sum_{i=1}^{4} w_i = 1$. Вагові коефіцієнти відображають відносну важливість відповідних складових і можуть визначатися політикою безпеки або класом захищеної мережі.

Для уникнення ситуації, коли подія з невалідною криптографічною перевіркою частково "компенсується" іншими складовими, вводиться жорстке обмеження:

$$Trust(E) = T_{crypto}(E) \cdot \big(w_2 T_{ctx}(E) + w_3 T_{time}(E) + w_4 T_{net}(E)\big), \quad (10)$$

що гарантує $Trust(E) = 0$ у разі провалу криптографічної верифікації. Така конструкція робить модель стійкою до ін'єкції подій, які намагаються пройти кореляцію за рахунок контекстної схожості без криптографічної доказовості.

Запропонована модель є повністю пояснюваною, оскільки внесок кожної складової в загальний рівень довіри може бути проаналізований окремо [13, 17]. На відміну від підходів, що базуються на непрозорих моделях машинного навчання, запропонована агрегація дозволяє явно простежити причини зниження або підвищення довіри до події та використовувати цю інформацію в механізмах прийняття рішень SIEM.

Таким чином, криптографічна модель формування рівня довіри до подій безпеки створює формальну основу для переходу від синтаксичної кореляції подій до інтелектуального формування мережевих інцидентів, у якому кожна подія оцінюється не лише за змістом, а й за ступенем її фактичної достовірності.

Інтелектуальне формування мережевих інцидентів на основі довіри до подій

У традиційних SIEM-системах формування інцидентів здійснюється шляхом кореляції подій за наперед визначеними правилами, часовими вікнами або шаблонами поведінки. При цьому ключовим критерієм ескалації зазвичай виступає кількість подій певного типу або їх повторюваність у заданому часовому інтервалі [22]. Такий підхід не враховує достовірність окремих подій і виходить із припущення, що всі події, які задовольняють умови правила, є рівнозначними з погляду довіри. У результаті формування інциденту часто відбувається на основі великої кількості подій низької якості, що призводить до хибних спрацьовувань і перевантаження аналітиків SOC.

У межах запропонованого підходу інцидент розглядається як результат інтелектуальної агрегації криптографічно оформлених тверджень про стан комп'ютерної мережі. Формування інциденту ґрунтується не на простому підрахунку подій, а на оцінюванні їх сукупної доказової сили з урахуванням рівня довіри та ризикової значущості кожної події [20, 22]. Формально інцидент визначається як:

$$Incident = f(E_1, \dots, E_n, Trust(E_i), Risk(E_i)), \quad (11)$$

де E_i – події безпеки, що потенційно пов'язані між собою, $Trust(E_i)$ – рівень довіри до події, визначений у попередньому розділі, $Risk(E_i)$ – оцінка ризику, яку подія становить для комп'ютерної мережі з урахуванням критичності активів і можливих наслідків. Оцінювання $Risk(E)$ може здійснюватися на основі статистичних і нейромережевих методів [15], здатних виявляти приховані закономірності та слабко виражені аномальні ознаки у потоках телеметричних даних.

Ключовою відмінністю від класичного підходу є те, що кожна подія вносить у формування інциденту не рівнозначний вклад, а зважений за рівнем її достовірності. Події з

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

низьким значенням $Trust(E)$ автоматично знижують свій вплив на результат кореляції або повністю виключаються з неї, якщо їх рівень довіри не перевищує мінімально допустимого порога. Таким чином, система стає стійкою до ін'єкції великої кількості формально коректних, але криптографічно недостовірних подій, які в традиційних SIEM могли б призвести до хибного інциденту.

Інтелектуальність запропонованого механізму проявляється в тому, що інцидент формується як узагальнене твердження, підтверджене сукупністю подій із високою довірою, навіть якщо їх кількість є відносно невеликою. Натомість велика кількість подій із низьким рівнем довіри не призводить до ескалації, оскільки їх сукупна доказова сила є недостатньою [10-11, 20]. Таким чином, відбувається перехід від кількісної логіки «більше подій – вищий пріоритет» до якісної логіки «більш достовірні події – вищий пріоритет».

Для формалізації цього підходу можна ввести агреговану оцінку підтвердження інциденту у вигляді:

$$Score_{inc} = \sum_{i=1}^{n} Trust(E_i) \cdot Risk(E_i), \quad (12)$$

де $Score_{inc}$ відображає сумарну доказову силу подій, що входять до потенційного інциденту. Інцидент вважається сформованим, якщо значення $Score_{inc}$ перевищує заданий поріг, який визначається політикою безпеки або класом захищеної мережі. Така схема дозволяє гнучко керувати чутливістю SIEM до різних типів загроз і адаптувати процес формування інцидентів до конкретних умов експлуатації.

Для забезпечення інтелектуальності механізму формування інцидентів вводиться "профіль доказовості" інциденту, який відображає внесок кожної події в підсумкову оцінку:

$$Contrib(E_i) = Trust(E_i) \cdot Risk(E_i), \quad (13)$$

Тоді інцидент супроводжується ранжованим набором $[Contrib(E_i)]$, що дозволяє сформувати пояснення рішення у вигляді: "які саме події стали ключовими доказами та чому" [13, 17]. Додатково якість сформованого інциденту можна оцінювати метрикою концентрації доказів:

$$Q_{inc} = \frac{\sum_{i=1}^{m} Contrib(E_i)}{\sum_{i=1}^{n} Contrib(E_i)}, \; m \ll n, \quad (14)$$

де E_i – події з найбільшим внеском. Високе значення Q_{inc} означає, що інцидент базується на небагатьох, але достовірних і ризиково значущих підтвердженнях, що зменшує "шумову" складову та підвищує аналітичну цінність інциденту для SOC.

На рис. 3 наведено послідовність обробки подій у SIEM: від криптографічної верифікації та обчислення $Trust(E)$ до кореляції кандидатів і прийняття рішення про ескалацію інциденту за порогом $Score_{inc} \geq \theta$.

Запропонований механізм також забезпечує пояснюваність процесу прийняття рішень, оскільки внесок кожної події в сформований інцидент може бути проаналізований окремо через значення $Trust(E_i)$ та $Risk(E_i)$ [17, 21]. Це дозволяє аналітикам SOC не лише бачити результат кореляції, а й розуміти, які саме події стали визначальними для ескалації інциденту та чому інші події були проігноровані або знецінені.

Таким чином, інтелектуальне формування мережевих інцидентів на основі довіри до подій забезпечує принципово новий рівень якості аналізу в SIEM [16-18, 21]. Запропонований підхід поєднує криптографічну перевірюваність подій із формалізованою оцінкою ризику, що дозволяє будувати інциденти як обґрунтовані та пояснювані твердження про стан безпеки комп'ютерної мережі, а не як механічний результат застосування кореляційних правил.

Алгоритм формування інцидентів у SIEM з урахуванням криптографічної довіри

Інтелектуальне формування мережевих інцидентів у запропонованій SIEM-моделі реалізується у вигляді послідовного алгоритмічного процесу, в якому кожна подія безпеки проходить етапи криптографічної верифікації, оцінювання довіри та зваженої кореляції [17,

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

19, 21]. Алгоритм орієнтований на потокову обробку подій і не потребує глобального аналізу всього масиву телеметрії, що робить його придатним для застосування в реальних корпоративних комп'ютерних мережах.

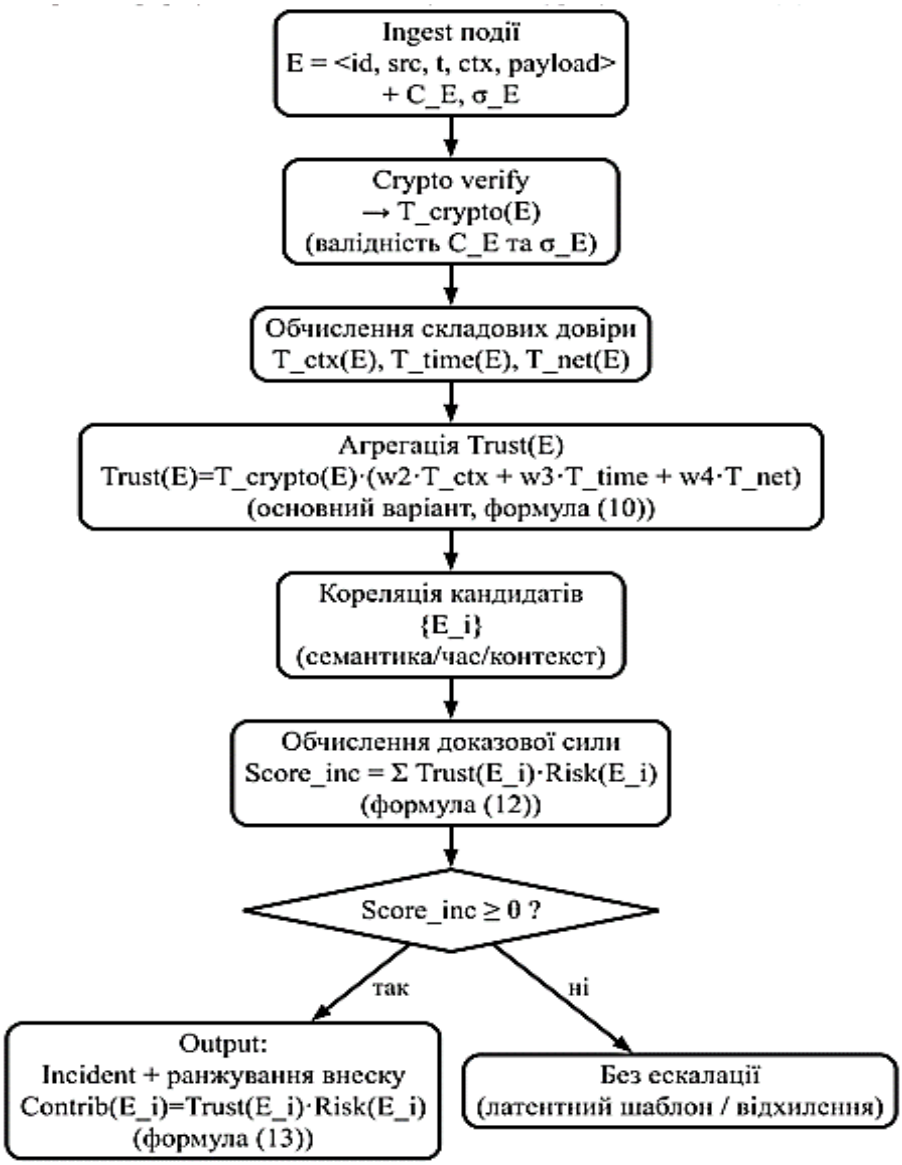

Рис. 3. Алгоритм формування мережевих інцидентів у SIEM на основі $Trust(E)$ та $Score_{inc}$

На першому етапі здійснюється прийом події E, яка надходить до SIEM із сенсора, агента або мережевого вузла. Подія розглядається у формалізованому вигляді $E = \langle id, src, t, ctx, payload \rangle$ разом із відповідним криптографічним зобов'язанням C_E та, за наявності, цифровим підписом σ_E [16-18]. На цьому етапі не робиться жодних припущень щодо достовірності події; вона розглядається як потенційне твердження про стан мережі.

Другий етап полягає у криптографічній верифікації події, під час якої перевіряється коректність зобов'язання C_E та валідність цифрового підпису σ_E. У разі виявлення порушення цілісності або автентичності подія відхиляється або маркується як така, що має нульовий рівень довіри [17, 19, 23]. Таким чином, події, які не задовольняють базові криптографічні вимоги, не потрапляють у подальший процес кореляції, що зменшує навантаження на наступні етапи аналізу.

На третьому етапі виконується обчислення рівня довіри до події $Trust(E)$ відповідно до моделі. Значення $Trust(E)$ формується шляхом агрегування складових криптографічної

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

верифікації, узгодженості контексту, часових характеристик та мережевих ознак [21]. Отримане значення є кількісною мірою достовірності події та використовується як основний зважувальний коефіцієнт у подальшій кореляції.

Четвертий етап полягає у кореляції подій. Події з ненульовим рівнем довіри групуються у потенційні кореляційні множини $\{E_1, \dots, E_n\}$ на основі семантичної близькості, часових зв'язків або спільного контексту. На відміну від класичних SIEM, у запропонованому алгоритмі події з низьким значенням $Trust(E)$ або зниженим коефіцієнтом узгодженості контексту мають істотно менший вплив на процес кореляції або повністю виключаються з нього за досягнення заданого порога.

На п'ятому етапі здійснюється формування інциденту шляхом обчислення агрегованої оцінки доказової сили подій: $Score_{inc} = \sum_{i=1}^{n} Trust(E_i) \cdot Risk(E_i)$. Інцидент вважається сформованим, якщо значення $Score_{inc}$ перевищує встановлений поріг ескалації. У протилежному випадку кореляційна множина зберігається як латентний шаблон або відкидається без генерації інциденту [16-18]. Таким чином, рішення про ескалацію ґрунтується не на кількості подій, а на сукупній якості та достовірності підтверджень.

З алгоритмічного погляду обробка кожної події виконується за сталий або лінійний час відносно кількості подій у поточному кореляційному вікні. Криптографічна верифікація та обчислення $Trust(E)$ мають складність $O(1)$, тоді як кореляція в межах ковзного вікна має складність $O(k)$, де k – кількість подій у відповідному часовому або контекстному сегменті. Формування інциденту шляхом обчислення $Score_{inc}$ також виконується за $O(k)$, що робить загальну складність алгоритму прийнятною для високонавантажених SIEM-систем.

Масштабованість запропонованого алгоритму забезпечується його потоковою природою та локальністю обчислень. Алгоритм не потребує глобальної перебудови графів подій або повторного аналізу всієї історії телеметрії, а працює з обмеженими кореляційними вікнами [21]. Це дозволяє ефективно розпаралелювати обробку подій, розподіляти навантаження між вузлами SIEM та застосовувати алгоритм у великих корпоративних і хмарних середовищах без деградації продуктивності.

Таким чином, запропонований алгоритм формування інцидентів поєднує криптографічну строгість із обчислювальною ефективністю, забезпечуючи практичну реалізовність інтелектуального підходу до аналізу подій безпеки в сучасних SIEM-системах.

Архітектура SIEM з підтримкою криптографічної довіри до подій

Запропонована криптографічна модель довіри до подій безпеки не вимагає радикальної перебудови існуючих SIEM-систем, а інтегрується в їх архітектуру у вигляді логічно відокремлених функціональних модулів [16-18, 23]. Це дозволяє зберегти традиційні механізми збору телеметрії та кореляції, водночас розширивши їх можливості за рахунок формалізованого оцінювання достовірності подій.

Архітектурно SIEM з підтримкою криптографічної довіри до подій складається з п'яти основних рівнів: рівня джерел подій, рівня попередньої криптографічної фіксації, рівня верифікації та оцінювання довіри, рівня інтелектуальної кореляції та рівня формування інцидентів і реагування.

На рівні джерел подій розташовані традиційні компоненти інфраструктури SIEM, зокрема мережеві сенсори, IDS/IPS, агенти кінцевих точок, системні журнали та хмарні сервіси. На цьому рівні події формуються у вигляді структурованих записів, доповнених контекстною інформацією, необхідною для подальшої обробки [12]. Важливо, що джерела подій не потребують знання повної моделі довіри; вони лише формують базове представлення події.

Рівень криптографічної фіксації подій реалізує формування криптографічного зобов'язання C_E та, за необхідності, цифрового підпису σ_E. Цей рівень може бути реалізований як частина агента збору подій або як окремий сервіс на вході в SIEM [23]. Його завданням є криптографічне зв'язування семантичного вмісту події, контексту та часових характеристик у

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

єдине перевірюване твердження. Таким чином, уже на ранньому етапі забезпечується захист події від непомітної модифікації або підміни.

Криптографічна фіксація подій створює формальну основу для подальшого кількісного оцінювання довіри до подій безпеки на вищих рівнях архітектури. Перевірюваність криптографічного зобов'язання дозволяє однозначно відокремити автентичні події від потенційно ін'єктованих або частково скомпрометованих тверджень ще до етапу кореляції. У поєднанні з контекстно-часовою узгодженістю це підвищує стійкість SIEM до атак маніпуляції подіями та забезпечує надійність подальшого аналізу інцидентів.

На рівні верифікації та оцінювання довіри відбувається перевірка цілісності та автентичності подій, а також обчислення рівня довіри $Trust(E)$ відповідно до криптографічної моделі. Цей рівень є концептуально новим для класичних SIEM-систем і відіграє роль фільтра якості подій [17, 23]. Події, що не проходять криптографічну верифікацію або мають критично низький рівень довіри, відсіюються ще до етапу кореляції, що істотно знижує навантаження на подальші компоненти.

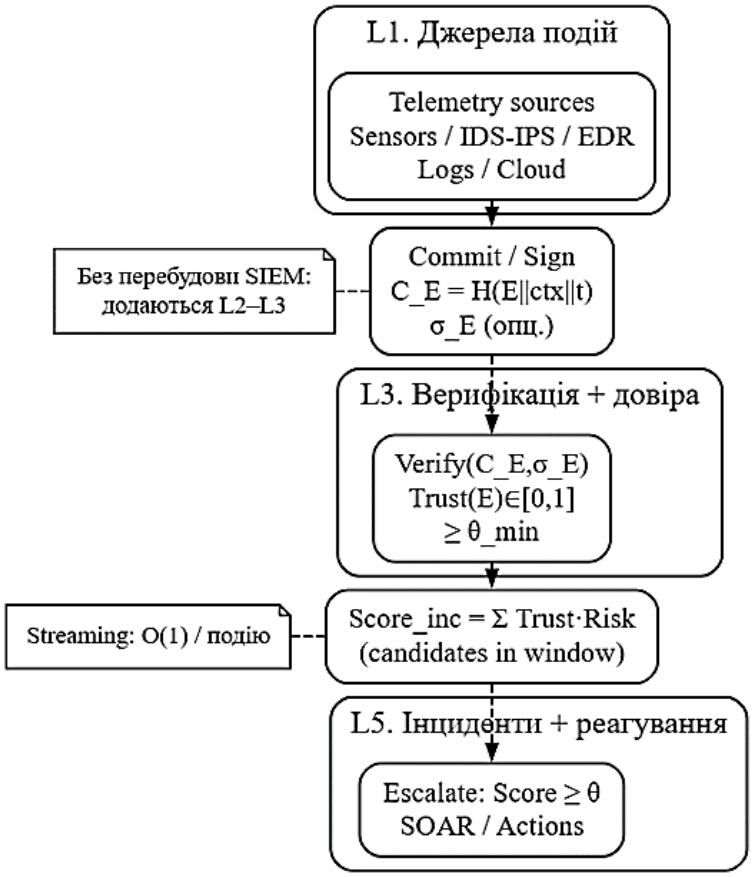

Рис. 4. Багаторівнева архітектура SIEM з інтегрованими механізмами криптографічної фіксації та оцінювання довіри до подій

Рівень інтелектуальної кореляції відповідає за групування подій у потенційні інциденти з урахуванням не лише семантичних і часових ознак, але й значень $Trust(E)$ та $Risk(E)$ [21]. На цьому рівні реалізується якісно нова логіка кореляції, у якій події з високою довірою мають пріоритетний вплив на формування інциденту, тоді як події з низькою довірою знижують свою вагу або виключаються з аналізу. Це дозволяє будувати кореляційні ланцюги, стійкі до шуму та навмисних маніпуляцій подіями. Додатково на цьому рівні може застосовуватися інтелектуальне оцінювання ризикової значущості подій на основі виявлення прихованих аномальних патернів у телеметричних даних із використанням статистичних і нейромережевих методів [15]. Це дає змогу адаптивно коригувати внесок окремих подій у

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

процес кореляції залежно від контексту мережі та динаміки загроз. У результаті формується більш компактний і доказово узгоджений набір подій, що підвищує аналітичну цінність інцидентів для подальшого реагування SOC.

На рівні формування інцидентів і реагування здійснюється остаточне прийняття рішень щодо ескалації інцидентів, їх пріоритизації та запуску сценаріїв реагування. Інциденти, сформовані на основі криптографічно перевірених подій із високою довірою, можуть автоматично передаватися до систем SOAR, механізмів ізоляції вузлів або політик доступу [21]. Завдяки пояснюваній природі моделі аналітики SOC можуть бачити, які саме події та з яким рівнем довіри стали підставою для ескалації. Важливою перевагою запропонованої архітектури є її модульність і масштабованість [23]. Кожен рівень може бути реалізований незалежно та розгорнутий у розподіленому середовищі. Криптографічна фіксація та верифікація подій легко паралелізуються, а оцінювання довіри не потребує глобального стану системи. Це дозволяє інтегрувати модель у великі SIEM-інсталяції без суттєвого впливу на продуктивність. Загальну архітектуру SIEM з підтримкою криптографічної довіри до подій наведено на рис. 4, де показано логічне розділення системи на рівні джерел подій, криптографічної фіксації, верифікації та оцінювання довіри, інтелектуальної кореляції [23], а також формування інцидентів і реагування.

Таким чином, архітектура SIEM з підтримкою криптографічної довіри до подій забезпечує логічне завершення запропонованого підходу, поєднуючи криптографічну строгість, інтелектуальну кореляцію та практичну реалізовність [23]. Вона демонструє, що довіра до подій може бути впроваджена як системна властивість SIEM, а не як зовнішній або допоміжний механізм.

Обговорення результатів та переваг підходу

Запропонований підхід до формування мережевих інцидентів у SIEM на основі криптографічної довіри до подій забезпечує низку принципових переваг порівняно з класичними механізмами кореляції, що безпосередньо впливають на якість виявлення загроз і ефективність роботи команд SOC [21]. Ключовою відмінністю є перехід від кількісної оцінки подій до якісної оцінки їх достовірності, що змінює саму логіку прийняття рішень у SIEM.

Однією з основних практичних переваг запропонованого підходу є суттєве зменшення кількості хибних спрацьовувань (false positives). У традиційних SIEM хибні інциденти часто формуються внаслідок накопичення великої кількості подій, які формально задовольняють умови кореляційного правила, але не відображають реального порушення безпеки. У запропонованій моделі події з низьким рівнем довіри автоматично знижують свій внесок у процес формування інциденту або повністю виключаються з нього. Це означає, що шумові, повторні або частково скомпрометовані події не призводять до ескалації, навіть якщо їх кількість є значною. У результаті SIEM формує меншу кількість інцидентів, але з вищою доказовою якістю.

Згідно з табл. 1, Crypto-Trust SIEM підвищує точність формування інцидентів (Precision) з 0.72 до 0.86, що відповідає збільшенню на 19.4%.

Таблиця 1

Порівняння Baseline SIEM та Crypto-Trust SIEM за метриками якості формування інцидентів

Метрика	*Baseline SIEM*	*Crypto-Trust SIEM*	*Зміна відносно Baseline*
Точність (Precision)	0.72	0.86	збільшення на 19.4%
Концентрація доказів інциденту $\boldsymbol{Q_{inc}}$	0.58	0.77	збільшення на 32.8%
Кількість інцидентів за добу	120	78	зменшення на 35.0%
Середня кількість подій на інцидент	3.1	6.8	зростання у 2.2 раза
Частка подій із низьким рівнем довіри	41%	18%	зменшення на 23 відсоткові пункти

Одночасно зростає концентрація доказів інциденту Q_{inc} з 0.58 до 0.77 (збільшення на 32.8%), а кількість інцидентів за добу зменшується з 120 до 78 (зменшення на 35.0%). Частка

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

подій із низьким рівнем довіри скорочується з 41% до 18%, що відповідає зменшенню на 23 відсоткові пункти та підтверджує пригнічення “шумових” подій до етапу ескалації.

Табл. 1 демонструє, що використання криптографічно зваженої довіри до подій підвищує не лише точність і доказову узгодженість інцидентів, а й їхню структурну насиченість. Зменшення частки подій з низьким рівнем довіри свідчить про ефективне пригнічення шуму на етапі кореляції.

На рис. 5 результати подано у нормалізованому вигляді (відносно Baseline SIEM), що дозволяє коректно зіставити метрики різної розмірності в межах єдиної 2D-візуалізації.

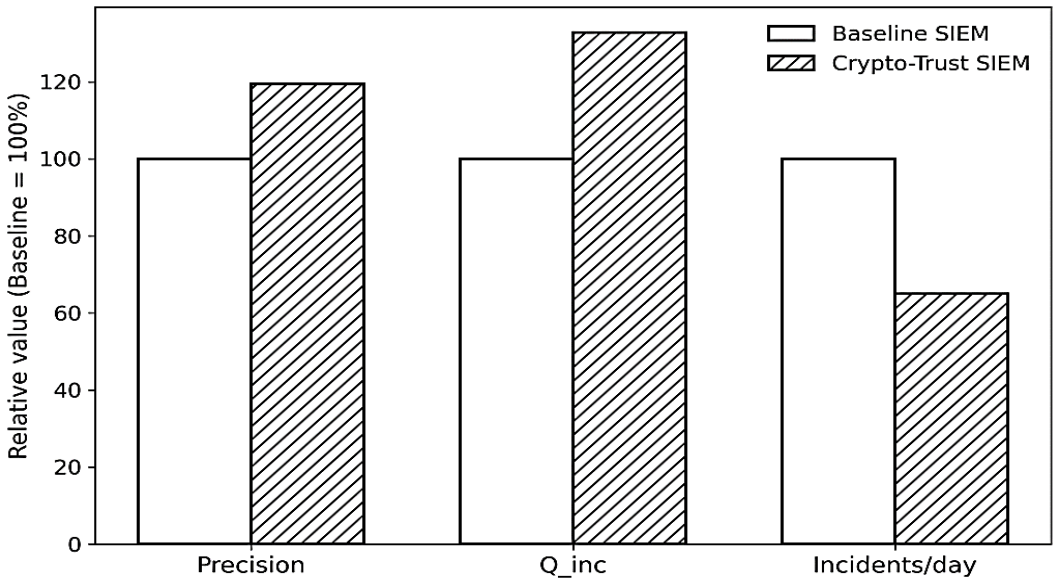

Рис. 5. Порівняння Baseline SIEM та Crypto-Trust SIEM за нормалізованими метриками якості формування інцидентів (Baseline = 100%): точність (Precision), концентрація доказів Q_{inc} та кількість інцидентів за добу (за даними табл. 1)

Запропонований підхід підвищує стійкість SIEM до атак ін’єкції подій, унеможливлюючи маніпуляції кореляцією за рахунок криптографічної верифікації та перевірки контекстно-часової узгодженості кожної події. Ін’єктовані або змінені події мають низький рівень довіри та не впливають на формування інцидентів, що забезпечує захист навіть у разі часткової компрометації джерел телеметрії.

Крім того, модель підвищує якість інцидентів, розглядаючи їх як узагальнені твердження, підтверджені сукупністю подій із високим рівнем довіри, що спрощує аналіз і пояснення для аналітиків SOC. Інтеграція довіри з оцінкою ризику забезпечує ефективну пріоритизацію інцидентів за їх доказовою силою та реальною загрозою для активів [12, 23]. При цьому ризикова складова може уточнюватися інтелектуальними статистичними та нейромережевими моделями, які виділяють приховані аномальні структури у телеметрії та підсилюють обґрунтованість пріоритизації інцидентів [15]. У цілому, інтеграція криптографічної довіри до подій переводить SIEM від механічної кореляції до інтелектуального аналізу інцидентів, зменшуючи хибні спрацьовування та підвищуючи стійкість у динамічних недовірених мережевих середовищах.

Висновки

У роботі запропоновано та науково обґрунтовано новий підхід до формування мережевих інцидентів у системах управління подіями та інцидентами інформаційної безпеки, який базується на криптографічній моделі довіри до подій безпеки. На відміну від традиційних SIEM-рішень, у яких події розглядаються як апріорно достовірні елементи аналізу, запропонований підхід трактує подію як криптографічно оформлене твердження про стан

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

комп'ютерної мережі, достовірність якого може бути формально перевірена та кількісно оцінена.

У межах дослідження сформульовано концептуальну постановку задачі довіри до подій безпеки в SIEM та введено новий об'єкт аналізу — рівень довіри до події. Запропоновано формалізоване подання події з урахуванням її семантичного вмісту, контексту генерації та часових характеристик, а також механізм криптографічного зобов'язання, що забезпечує перевірюваність цілісності й походження подій. На цій основі розроблено криптографічну модель формування рівня довіри, яка інтегрує результати криптографічної верифікації, узгодженість контексту, часову актуальність і мережеві ознаки подій у єдину пояснювану кількісну характеристику.

Ключовим результатом роботи є розроблення інтелектуального механізму формування мережевих інцидентів, у якому кореляція подій виконується з урахуванням їх доказової сили, а не лише кількості або формальної відповідності правилам. Показано, що запропонований підхід дозволяє суттєво зменшити кількість хибних спрацьовувань, підвищити стійкість SIEM до атак, спрямованих на ін'єкцію або підміну подій, та покращити якість сформованих інцидентів із погляду їх пояснюваності та практичної цінності для аналітиків SOC.

Розроблено алгоритм формування інцидентів з урахуванням криптографічної довіри, який має прийнятну обчислювальну складність і є масштабованим для застосування в корпоративних і розподілених мережевих середовищах. Запропонована архітектура SIEM з підтримкою довіри до подій демонструє можливість практичної інтеграції моделі в існуючі системи без необхідності кардинальної перебудови інфраструктури збору телеметрії.

Перспективи подальших досліджень пов'язані з розширенням і поглибленням запропонованої моделі в кількох напрямах. Зокрема, доцільним є дослідження адаптивних механізмів налаштування вагових коефіцієнтів складових довіри залежно від типу мережі, класу активів або поточного рівня загроз. Окремий інтерес становить інтеграція моделі криптографічної довіри з системами автоматизованого реагування (SOAR) та політиками доступу, що дозволить реалізувати замкнений контур прийняття рішень на основі перевірених подій. Подальші дослідження також можуть бути спрямовані на експериментальну валідацію запропонованого підходу в реальних або тестових середовищах, зокрема з використанням промислових SIEM-платформ і синтетичних сценаріїв атак. Перспективним є вивчення можливостей застосування запропонованої моделі в гетерогенних і недовірених середовищах, таких як хмарні інфраструктури та мережі з нульовою довірою (Zero Trust), де питання достовірності подій безпеки є особливо критичним.

Таким чином, результати роботи створюють теоретичне та практичне підґрунтя для розвитку SIEM нового покоління, у яких довіра до подій стає системною властивістю, а формування інцидентів ґрунтується на криптографічно перевірених і пояснюваних твердженнях про стан безпеки комп'ютерних мереж.

Перелік посилань

1. 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.

2. Soriano-Salvador, E., & Guardiola-Múzquiz, G. (2021). SealFS: Storage-based tamper-evident logging. Computers & Security, 108, Article 102325. https://doi.org/10.1016/j.cose.2021.102325.

3. Guardiola-Múzquiz, G., & Soriano-Salvador, E. (2023). SealFSv2: Combining storage-based and ratcheting for tamper-evident logging. International Journal of Information Security, 22, 447–466. https://doi.org/10.1007/s10207-022-00643-1.

4. Reijsbergen, D., Maw, A., Yang, Z., Dinh, T., & Zhou, J. (2022). TAP: Transparent and privacy-preserving data services (arXiv:2210.11702). https://doi.org/10.48550/arXiv.2210.11702.

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

6. Maosa, H., Ouazzane, K., & Ghanem, M. C. (2024). A hierarchical security event correlation model for real-time threat detection and response. Network, 4(1), 68–90. https://doi.org/10.3390/network4010004.

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

7. Velásquez, J. M. L., Monterrubio, S. M. M., Crespo, L. E. S., et al. (2025). SIEM-SC initial assessments: Towards a sustainable and compliant proposal for security information and event management. International Journal of Information Security, 24, Article 195. https://doi.org/10.1007/s10207-025-01109-w.

8. Uccello, F., Pawlicki, M., D'Antonio, S., Kozik, R., & Choraś, M. (2024). Effective rules for a rule-based SIEM system in detecting DoS attacks: An association rule mining approach. In D. S. Huang, P. Premaratne, & C. Yuan (Eds.), Applied intelligence (Communications in Computer and Information Science, Vol. 2015). Springer. https://doi.org/10.1007/978-981-97-0827-7_21.

9. 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. https://doi.org/10.1145/3695462.

10. 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.

11. 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(3), Article 18. https://doi.org/10.1145/3510581.

12. Usman, N., Usman, S., Khan, F., Jan, M. A., Sajid, A., Alazab, M., & Watters, P. (2021). Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics. Future Generation Computer Systems, 118, 124–141. https://doi.org/10.1016/j.future.2021.01.004.

13. Kostiuk, Y., Skladannyi, P., Sokolov, V., & Vorokhob, M. (2025). Models and technologies of cognitive agents for decision-making with integration of artificial intelligence. In Proceedings of the Modern Data Science Technologies Doctoral Consortium (MoDaST 2025) (pp. 82–96). CEUR-WS.

14. Li, Z., Chen, Q. A., Yang, R., Chen, Y., & Ruan, W. (2021). Threat detection and investigation with system-level provenance graphs: A survey. Computers & Security, 106, Article 102282. https://doi.org/10.1016/j.cose.2021.102282.

15. Kostiuk, Y., Skladannyi, P., Khorolska, K., Sokolov, V., & Hulak, H. (2025). Application of statistical and neural network algorithms in steganographic synthesis and analysis of hidden information in audio and graphic files. In Proceedings of the Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC 2025) (pp. 45–65). CEUR-WS.

16. Li, J., et al. (2022). LogKernel: A threat hunting approach based on behaviour provenance graph and graph kernel clustering. Security and Communication Networks, Article 4577141. https://doi.org/10.1155/2022/4577141.

17. Kostiuk, Y. (2025). Multi-agent system for detecting and counteracting attacks on the enterprise information system. In Insider threats and security in corporations (pp. 205–232). https://doi.org/10.36690/ITSC-205-232.

18. Wei, R., Cai, L., et al. (2021). DeepHunter: A graph neural network based approach for robust cyber threat hunting (arXiv:2104.09806). https://arxiv.org/abs/2104.09806.

19. Skladannyi, P., Kostiuk, Y., Rzayeva, S., & Mazur, N. (2025). Parallel data processing in extensible hash structures and performance evaluation. Cybersecurity: Education, Science, Technique, 3(31), 242–269. https://doi.org/10.28925/2663-4023.2025.31.1015.

20. Levshun, D., & Kotenko, I. (2023). Intelligent graph-based correlation of security events in cyber-physical systems. In S. Kovalev, I. Kotenko, & A. Sukhanov (Eds.), Proceedings of the Seventh International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'23) (Lecture Notes in Networks and Systems, Vol. 777). Springer. https://doi.org/10.1007/978-3-031-43792-2_12.

21. Lee, J., Kim, J., Kim, I., & Han, K. (2019). Cyber threat detection based on artificial neural networks using event profiles. IEEE Access, 7, 165607–165626. https://doi.org/10.1109/ACCESS.2019.2953095.

22. Jha, G. (2025). Security information and event management (SIEM). In Securing the enterprise. Apress. https://doi.org/10.1007/979-8-8688-1654-3_14.

23. Skladannyi, P. M., Hulak, H. M., & Kostiuk, Y. V. (2025). Generator of chaotic numbers with fuzzy control for cryptographic systems with dynamic trust. Telecommunication and Information Technologies, 4(89), 137–147. https://doi.org/10.31673/2412-4338.2025.048916.

Надійшла до редакції (Received): 14.02.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

http://creativecommons.org/licenses/by/4.0/
This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.

© Костюк Ю.В., Складанний П.М. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393