КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.618
УДК 004.7

**Смірнова Тетяна Віталіївна**
к.т.н., доцент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0000-0001-6896-0612
*sm.tetyana@gmail.com*

**Константинова Лілія Володимирівна**
викладач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0000-0002-3305-2427
*liliyashel1976@gmail.com*

**Конопліцька-Слободенюк Оксана Костянтинівна**
викладач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0000-0001-9981-5194
*ksuha80@gmail.com*

**Козлов Ян Олександрович**
студент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0009-0006-1617-4074
*kozlov.yan1@gmail.com*

**Кравчук Оксана Вікторівна**
інспектор відділу кадрів
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0009-0008-8453-0557
*vov-14@i.ua*

**Козірова Наталія Леонідівна**
асистент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0009-0005-8753-5132
*natalidonchenko23@gmail.com*

**Смірнов Олексій Анатолійович**
д.т.н., професор, завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет,
Кропивницький, Україна
ORCID ID: 0000-0001-9543-874X
*dr.smirnovoa@gmail.com*

# ДОСЛІДЖЕННЯ СУЧАСНОГО СТАНУ SIEM-СИСТЕМ

**Анотація.** У цій роботі проведено дослідження SIEM-систем, актуальність застосування яких значно виросла під час повномасштабного вторгнення росії в Україну. Було вирішено завдання з пошуку найбільш оптимальних рішень відповідно до наступних критеріїв: зручність використання, здатність інтегруватися з іншими рішеннями захисту, цінова політика та особливості. Для цього у роботі розглянуто загальний опис будови та принцип

функціонування системи SIEM, визначені можливості та особливості сучасних SIEM-систем, проведено дослідження наступного програмного забезпечення (ПЗ): Splunk Enterprise Security (Splunk), Elastic Security, IBM QRadar SIEM, Wazuh SIEM, Microsoft Sentinel. У результаті дослідження виявлено наступне: сучасні SIEM-рішення дозволяють автоматизувати частину процесів з виявлення та реагування на події безпекового характеру, дозволяють брати під контроль гібридні типи інфраструктури, які можуть включати хмарні середовища, системи віртуалізації та контейнеризації, робочі станції та інші корпоративні пристрої. Вони реалізуються як у вигляді розгортання своїх рішень на власних потужностях, так і у вигляді оренди відповідних ресурсів, надаючи послугу Software-as-a-Service. При цьому наявність великої кількості інтеграцій з різноманітними пакетами ПЗ та системами дозволяє SIEM стежити за відповідністю наявного стану кіберзахисту інформаційної інфраструктури організації певним міжнародним стандартам, як то ISO 27001, GDPR чи PCI DSS. Визначено, що у сучасних SIEM для виявлення аномалій у поведінці систем та користувачів, а також для пріоритизації виявлених вразливостей та пропонування кроків щодо покращення стану кіберзахисту використовуються досягнення у сферах машинного навчання та штучного інтелекту. Розглянуті рішення працюють сумісно з іншими сучасними системами, як то SOAR чи EDR/XDR, що підвищує ефективність SIEM-систем та, як наслідок, операційних центрів безпеки, тому, на думку авторів, відповідні технології заслуговують на подальше дослідження.

**Ключові слова:** SIEM; управління інформацією та подіями безпеки; хмарні платформи; критична інфраструктура; кібербезпека; інформаційна безпека.

## ВСТУП

**Постановка завдання дослідження.** За даними Державної служби спеціального зв'язку та захисту інформації України, в складі якої функціонує CERT (англ. Computer Emergency Response Team — команда реагування на комп'ютерні надзвичайні події), кількість ворожих кібератак на Україну зросла втричі у порівнянні з 2021 роком. Під атаки підпадають як медіаресурси, так і об'єкти критичної інфраструктури [1]. Така тенденція підтверджує необхідність запровадження систем забезпечення кібербезпеки на організаційному та технічному рівні в уразливих установах.

Існує багато принципово різних рішень для захисту інформаційно-комунікаційних систем: мережеві екрани, системи виявлення та запобігання вторгненням (IDS/IPS), антивіруси; але лише їх недостатньо для вчасного реагування на загрози або шкідливі дії. На момент, коли спеціаліст виявить джерело порушень та сформує можливі способи протидії — розмір шкоди може стати занадто великим. Саме для пришвидшення процесів, необхідних для захисту системи, створюються спеціальні операційні центри безпеки (англ. SOC, Security Operation Center), основним компонентом котрих є SIEM-системи. Управління подіями безпеки (SIEM, Security Information and Event Management) є важливим компонентом будь-якого центру безпеки чи програми кібербезпеки для організації. Аналітики безпеки покладаються на допомогу SIEM, яка корелює журнали та надійно ідентифікує будь-які підозрілі дії в їхній інфраструктурі, щоб вони могли негайно реагувати на будь-які загрози чи атаки. SIEM — це комбінація керування інформацією про безпеку (SIM) — збір даних журналу, подій; і управління подіями безпеки (SEM) — моніторинг і оповіщення в реальному часі [2].

SIEM-системи стають сполучною ланкою між іншими рішенням захисту, що дозволяє не тільки зберігати усю безпекову інформацію в одному місці, але й тим самим збагачувати аналітику, контролювати стан усіх елементів системи та виявляти несанкціоновані дії у реальному часі.

**Постановка проблеми.** Зважаючи на те, що після запровадження SIEM-система стає основним елементом системи захисту інформаційної інфраструктури організації та, за сумісництвом, основним робочим середовищем спеціаліста із забезпечення кібербезпеки, постає завдання з пошуку найбільш оптимальних рішень відповідно до наступних критеріїв: зручність використання, здатність інтегруватися з іншими рішеннями захисту, цінова політика та особливості. Дослідження існуючих рішень відповідно до заданих критеріїв дає можливість оцінити їх в повній мірі для обрання більш оптимального варіанту.

**Аналіз останніх досліджень і публікацій.** В роботах [2] – [5] розглядаються основні рішення SIEM-систем та їхня роль у забезпеченні інформаційної безпеки, але, на думку авторів цієї статті, дані дослідження не повною мірою охоплюють сучасні рішення, особливо вільні з відкритим кодом, та можливості таких систем. Таким чином, дослідження сфокусоване на аналізі існуючих пропозицій та актуальних можливостей SIEM-систем.

**Мета статті.** Дослідити структуру та принцип роботи SIEM-систем, можливості запровадження їх у різнотипних організаціях, актуалізувати перелік лідерів та визначити місце систем з відкритим кодом серед поширених рішень. Проаналізувати вплив сучасних досягнень у розвитку інформаційних технологій на SIEM-системи, використання хмарних ресурсів, машинного навчання та інтеграцію із сучасними системами безпеки.

## ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

### Опис будови та принцип функціонування системи SIEM

За визначенням, SIEM — це програмне забезпечення, яке дозволяє отримувати дані з безпеки інформаційно-комунікаційних систем та відображати їх як корисну інформацію в одному місці. Фактично, такі системи поєднують у собі два старіші рішення: SIM (Security Information Management — управління інформацією безпеки) та SEM (Security Events Management — управління подіями безпеки), що має сенс через спільне походження даних [2].

SIEM, як моніторингова система, інтегрує різноманітні надбудови для аналізу в основному безпекових даних. Проте, як будь-яка інша система моніторингу, вона може збирати та візуалізувати метрики та журнали подій, які не обов'язково стосуються безпеки, але вказують на загальний стан системи. Завдяки потужним інструментам візуалізації фахівці можуть краще аналізувати стан системи, швидше виявляти аномалії та ефективно реагувати на можливі загрози, які можуть призвести до такого некоректного функціонування.

Як було вказано раніше, SIEM-системи виступають як сполучна ланка в системах безпеки, проте вони самі по собі не сприяють поліпшенню так званої «безпекової постави» організації, що означає рівень захисту та готовність до реагування на загрози. Сучасні рішення, такі як Splunk Enterprise Security, [10] Elastic Security, [12] або IBM QRadar, [15] мають широкий спектр плагінів для інтеграції з різноманітними системами захисту, включаючи журнали аудиту кінцевих точок (такі як персональні комп’ютери, віртуальні машини, контейнери та ін.), окремі веб-сервіси та бази даних, мережеві пристрої, мережеві екрани, сканери вразливостей, системи виявлення та запобігання вторгнень, хмарні ресурси, розвідку про кіберзагрози та інше.

Стандартні протоколи логування, такі як Syslog, які доступні за замовчуванням у більшості операційних систем, мають можливість віддаленого логування. У цьому випадку журнали аудиту, незалежно від того, чи зберігаються вони локально, пересилаються до центрального хабу, який відповідає за їх обробку та зберігання. Хоча елементи інформаційної системи можуть використовувати стандартні протоколи логування, для більшості з них розроблені спеціалізовані інтеграції у вигляді «агентів». Ці агенти збирають збагачені та більш актуальні дані, враховуючи їхню природу та існуючі вектори загроз, що робить їх більш оптимізованими під окремий компонент. Зазвичай вони також надають можливість більш тонкого налаштування спеціалістом.

Чим більше компонентів системи генерують дані безпеки, тим більш ефективною стає SIEM-система. Покрім моніторингу, важливим завданням будь-якої SIEM-системи є накопичення та уніфікація журналів аудиту безпеки, що також відоме як «керування журналами аудиту». З огляду на це, сучасні системи дозволяють працювати з розподіленими базами даних, реплікувати їх та контролювати термін зберігання даних, що відоме як «зберігання даних» (data retention). Ще одним елементом, який значно підвищує ефективність SIEM, є модуль збагачення журналів, який виконує попередню обробку журналів для виділення значущої інформації та нормалізації даних. Це покращує роботу модулів співставлення з заданими правилами та кореляції даних та подій [7].

Експерт, у свою чергу, володіє потужним інструментарієм для фільтрації журналів подій, формування змістовних послідовностей логів та, відповідно, отримання більш чіткого уявлення про загальний стан системи. Завдяки збагаченим даним, пошук закономірностей стає більш інтерактивним і, відповідно, ефективнішим. Аналізуючи послідовні логи, що вказують на наявність загрози, SIEM може автоматично генерувати сповіщення про виявлену загрозу та навіть автоматично виконувати дії для її ліквідації.

Окремим аспектом будь-якої сучасної SIEM-системи є наявність інформаційних панелей з візуалізованою інформацією про поточний стан системи, включаючи метрики завантаження ресурсів, кількість віддалених підключень та список адрес, з яких надходять найбільше запитів. Такі елементи дозволяють оперативно контролювати загальний стан інфраструктури в реальному часі з одного центрального місця.

Важливо зазначити, що кожний з елементів SIEM-системи може бути представлений окремим рішенням, що створює певну модульність системи: за умови наявної інтеграції з іншими елементами системи один рушій візуалізації (або будь-який інший елемент) може бути заміненим на інший. Деякі комбінації рішень краще інтегруються один з одним, інші потребують додаткової конфігурації, але без наявності хоча б однієї зі складових SIEM-система є неповноцінною.

**Можливості SIEM-систем**

Враховуючи тісний зв’язок SIEM-систем з роботою операційного центру безпеки (SOC), вони мають низку можливостей, що прискорюють реагування на кіберінциденти та покращують загальний стан кібербезпеки організації.

Перш за все, варто виділити такі функції SIEM-систем як агрегація та збагачення даних. Вони грають визначальну роль у будь-якому рішенні SIEM, адже якість даних впливає на усі наступні операції та на ефективність SOC. Централізація інформації з різних джерел полегшує інтеграцію відповідної системи в інфраструкурі інформаційно-комунікаційних систем організації будь-якого розміру.

Отже, SIEM виступає як центр контролю та управління безпекою системи. Загалом, ці характеристики роблять такі системи ідеальним середовищем для роботи фахівців із

швидким реагуванням на загрози та кіберінциденти. Різні джерела інформації можуть подавати її у різному форматі з акцентом на певні метрики чи події, або навіть не мати можливості налаштувати такі акценти, і тим самим надавати загальну інформацію, яка не прямо пов'язана з безпекою. У таких випадках SIEM-системи проводять нормалізацію даних та збагачують їх додатковою інформацією, отриманою як безпосередньо, так і через аналіз інших джерел даних.

Будучи технічним ядром SOC, SIEM виконує додаткову функцію — виявлення загроз. Робить вона це використовуючи правила, написані спеціалістами та засновані на перевірці певних умов, та поведінкову аналітику, яку генерує на базі наявних даних. Багато актуальних рішень надають можливість інтегрувати різні джерела «кіберрозвідки», яка містить перелік актуальних індикаторів компрометації. Підозрілі події можуть отримувати оцінку відповідно до глобально доступної бази знань про тактику та методи діяльності зловмисників, що має назву MITRE ATT&CK. Усе це надає можливість завчасно ідентифікувати підозрілу подію та в режимі реального часу сповістити про загрозу команду SOC [5].

Різні компанії можуть потребувати різного рівня захисту для різних ресурсів, зокрема даних, і цей рівень повинен відповідати певним стандартам. Відомі SIEM-системи дозволяють перевіряти відповідність наявного стану до таких міжнародних стандартів, як PCI-DSS (Payment Card Industry Data Security Standard — стандарт безпеки даних індустрії платіжних карток), HIPAA (Health Insurance Portability and Accountability Act — закон про мобільність та відповідальність у медичному страхуванні), GDPR (General Data Protection Regulation — загальний регламент про захист даних) та інші.

**Особливості сучасних SIEM-систем**

Аналіз сучасних рішень SIEM-системи показує, що хоч усі вони і мають спільні властивості та функції (навіть можуть інтегруватися одне з одним), кожне рішення поступово запроваджує передові рішення та технології у сфері інформаційних технологій загалом.

Через велику кількість різноманітних джерел сучасні SIEM-системи надають можливість інтегрувати практично будь-яке джерело, починаючи від окремих веб-ресурсів завершуючи мобільними пристроями. Також, через надмірну кількість даних, які мають зберігатися, все частіше використовуються розподілені бази даних. Цей підхід вирішує проблему централізації інформації, адже дані можуть зберігатися та реплікуватися більш гнучко, що робить систему більш стійкою. Однак доводиться більше уваги приділяти створенню політики зберігання даних, яка регламентує тривалість зберігання тих чи інших даних [3].

З розвитком машинного навчання різноманітні продукти включили його у свої функції — зокрема, аналіз патернів у великій кількості даних та покращення рекомендацій. SIEM-системи також використовують машинне навчання, оскільки велика кількість даних з однієї системи є сприятливим середовищем для навчання нейронних мереж виявляти аномалії у поведінці різних компонентів системи, які звичайно можуть залишитися непоміченими для звичайного спеціаліста (наприклад, підключення до системи у позаробочий час).

Крім того, не кожна організація може дозволити собі виділити достатньо апаратних ресурсів для цілодобової роботи системи, яка, за великим рахунком, не захищає організацію. Провідні SIEM-системи дозволяють розгортати відповідну інфраструктуру у хмарному середовищі, перетворюючи SIEM на сервіс. Це уникне фізичної ізоляції внутрішньої частини інформаційної системи, пов'язуючи її з хмарним середовищем, і

водночас збереже усі переваги SIEM-системи, а за належної конфігурації навіть нейтралізує недоліки. Цей підхід також є оптимальним, якщо частина компонентів інформаційної системи розташована в хмарі, оскільки популярні SIEM-системи мають широкі можливості інтеграції з основними хмарними провайдерами.

Як зазначено раніше, більшість розроблених SIEM-систем постачаються з агентами для кінцевих точок. Ці агенти можуть не лише відправляти необхідну інформацію на сервер, а й виконувати роль антивірусу чи сканера вразливостей локального хоста, а також автоматично ізолювати уражені хости від мережі у випадку виявлення загрози, що забезпечує безпеку решти системи. Це частина підходу SOAR (Security Orchestration, Automation and Response — оркестрація, автоматизація та реагування безпеки). Такий підхід частково зменшує вплив людського фактору у перші секунди після виявлення кіберінциденту, виконуючи попередні дії з реагування. Наявність агентів також дозволяє збирати «аналітику поведінки користувачів та сутностей» (англ. User and Entity Behavior Analytics), що допомагає швидше виявляти аномалії, які можуть бути результатом потенційно зловмисної активності та контролювати додатковий вектор атак [8].

У випадку кібератаки SOC-аналітики після реагування на кіберінцидент мають з'ясувати, яким чином відбулася кібератака та які ресурси було уражено. Зазвичай це займає багато часу через велику кількість даних. Сучасні рішення дозволяють автоматично будувати часовий графік атаки та представляти її у візуальному вигляді, пришвидшуючи процес аналізу та покращуючи його результати.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

З метою всебічного огляду наявного ринку SIEM-систем далі буде порівняно рішення корпоративного рівня та рішення з відкритим кодом, збалансовані рішення та такі, що мають вузьку спеціалізацію або певні значущі особливості. Більшість розглянутих рішень включені до звіту «магічного квадранту SIEM-систем» дослідницького центру Gartner [5], який щорічно формує список поширених SIEM-систем та виділяє серед них лідерів ринку, нішевих гравців та ін.

**Splunk Enterprise Security (Splunk)**

Splunk займає лідируючі позиції на ринку SIEM-систем за версією Gartner [9] та займає близько 30% частки ринку SIEM-систем.

Це рішення надає можливість отримання, індексування та візуалізації даних для моніторингу подій, пов'язаних з безпекою. Splunk надає просунуту аналітику у сфері безпеки, що включає машинне навчання без нагляду та поведінковий аналіз користувачів.

Незважаючи на це, дане рішення має дуже загальні заздалегідь визначені правила кореляції для моніторингу та звітування. До того ж, вбудований функціонал реагування обмежене лише сповіщеннями електронною поштою. Однак, через модульну природу SIEM-систем усі недоліки компенсуються величезною кількістю інтеграцій та плагінів, які заздалегідь налаштовані для певних задач та надають можливість автоматизації різноманітних повторюваних задач [10].

Splunk може бути розгорнуто як на локальних обчислювальних потужностях, так і у віртуальних машинах, у хмарному середовищі та навіть у вигляді SaaS (Software-as-a-Service) за допомогою Spunk Cloud, що дає змогу мінімізувати розмір інфраструктури. Таким чином, Splunk розрахований на організації будь-якого розміру, до того ж цінова політика розраховується залежно від кількості даних, які обробляються SIEM-системою [11].

**Elastic Security**

Elastic Security входить до стеку технологій Elastic Stack, який включає елементи з відкритим кодом, як то: розподілена база даних Elasticsearch, модуль збагачення журналів подій Logstash, рушій візуалізації Kibana, агенти Beats та інше.

Зазвичай, даний стек технологій використовується для розгортання системи моніторингу інфраструктури та окремих додатків. Дане рішення має більш гнучку систему створення правил та повідомлень про знайдені в реальному часі збіги з правилами, тож може використовуватись як SIEM-система [12].

Elastic Stack також має пропрієтарну ліцензію, яка додає до системи можливість використання машинного навчання для пошуку аномалій, а також модуль Elastic Security, який виступає просунутим агентом на важливих об'єктах інформаційної інфраструктури та дозволяє аналізувати дані одразу та об'єктах та вчасно реагувати на загрози [13]. Також цей модуль дозволяє аналітикам візуально простежити за подіями, пов'язаними з певною загрозою та швидше знаходити початкову точку проникнення загрози в інфраструктуру та елементи системи, які зазнали впливу [14].

Серед недоліків Elastic Stack зазначають обмежену кількість інтеграцій та розрахунок системи на DevOps-практики, тож підходить це рішення, переважно, організаціям, так чи інакше пов'язаним з розробкою програмного забезпечення. Безкоштовне рішення знаходиться поміж рішеннями моніторингу та SIEM-системами, у той час як ліцензовані можливості виводять Elastic Stack на спільний рівень зі Splunk [5].

**IBM QRadar SIEM**

IBM QRadar Security Intelligence Platform складається з декількох продуктів, спрямованих на забезпечення безпеки інформаційної інфраструктури корпоративного рівня: QRadar SIEM, ядро платформи що відповідає за агрегацію та аналіз даних і сповіщення про загрози, QRadar SOAR для автоматизації реагування на певні загрози, QRadar EDR для захисту кінцевих точок від атак «нульового дня» (англ. zero-day attacks) та QRadar Log Insights, оптимізований для аналізу великої кількості даних в хмарному середовищі [15].

Окрім наявної екосистеми QRadar SIEM відрізняється просунутими у порівнянні з більшістю SIEM-системами засобами аналізу, пріоритизації та кореляції даних із застосуванням машинного навчання та ШІ. Це дає змогу SIEM виявляти більш актуальні загрози, порівнюючи їх з наявними джерелами кіберрозвідки, та оцінювати їхню критичність та терміновість. Інтеграція з базами знань методологій кібератак MITRE ATT&CK дає змогу пропонувати можливі кроки реагування на загрозу, а також відновлювати послідовність подій окремої атаки, знаходячи зв'язок між подіями та аналізуючи їх у контексті матриці тактик та технік зловмисників [16].

Надаючи доступ до магазину плагінів, IBM QRadar SIEM може інтегруватися з великою кількістю додатків та вендорів, що у поєднанні з машинним навчанням дозволяє створювати базову лінію поведінки користувачів та помічати аномальні події.

Крім того, ця платформа містить заздалегідь налаштовані конфігураційні набори та правила, які відповідають вимогам таких стандартів, як HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation), FISMA (Federal Information Security Management Act), SOX (Sarbanes-Oxley), ISO 27001, PCI DSS (Payment Card Industry Data Security Standard) та інші [17].

Відповідність світовим безпековим стандартам у поєднанні з гнучкістю щодо розміру та середовища інфраструктури (on-premise, хмарне чи гібридне) робить це

рішення переважно застосовним до великих корпоративних інфраструктур, що впливає на цінову політику продукту.

**Wazuh SIEM**

Wazuh — це платформа для безпекового моніторингу та захисту інформаційної інфраструктури та ресурсів, яка розвивається за допомоги спільноти та складається з рішень з відкритим кодом. Платформа орієнтована за захист цифрових активів та покращення безпекової постави організації [18].

Платформу Wazuh було повністю інтегровано в Elastic Stack [19], тому це рішення можна вважати вільною альтернативою Elastic Security. Також елементи Wazuh можуть бути інтегрованими в SIEM Splunk.

Wazuh SIEM, як і інші рішення, надає змогу аналізувати журнали безпеки, генерувати сповіщення та попередження на основі певних правил. Це рішення дозволяє підключати різноманітні джерела ідентифікаторів компрометації, що робить його достатньо гнучким. Як і SIEM-системи корпоративного рівня, Wazuh має певну кількість попередньо налаштованих панелей та правил, які роблять його відповідним до таких стандартів, як PCI DSS, NIST 800-53, GDPR, TSC SOC2 та HIPAA [20].

На ряду з пошуком вразливостей, дана SIEM-система надає змогу знаходити вразливі конфігурації та вади безпеки в інформаційній інфраструктурі та порівнювати відповідність наявного стану її захищеності кращим практикам та стандартам у сфері кібербезпеки, що є важливим вектором атак та за замовчуванням не моніториться більшістю SIEM-систем [21].

У поєднанні з XDR-рішенням Wazuh дає змогу також виявляти шкідливе ПЗ, слідкувати за цілісністю окремих файлів, оперативно реагувати на кіберінциденти та стежити за безпекою систем, розгорнутих у системних контейнерах. Wazuh може захищати обчислювальні потужності у хмарному середовищі та оцінювати загальний стан захищеності інформаційної інфраструктури та створювати змістовні звіти відповідного характеру.

Програмний код платформи розповсюджується з ліцензією GNU GPL2, що дозволяє безкоштовно використовувати його у комерційних та некомерційних цілях [22]. Засновники цієї системи також розповсюджують її як SaaS у вигляді Wazuh Cloud.

**Microsoft Sentinel**

У звіті дослідження «2022 Gartner Magic Quadrant for SIEM report» [5] лідером у галузі SIEM-систем було визнано Microsoft Sentinel. Це рішення представляє собою об’єднану платформу забезпечення безпеки операцій, яка поєднує можливості управління захистом інформації (SIEM), розширеного виявлення та реагування (XDR) і автоматизації, оркестрації засобів безпеки та реагування на кіберінциденти (SOAR) [23].

Sentinel орієнтований на хмарне середовище, але може бути адаптованим під гібридну інфраструктуру. Це рішення особливо ефективне за наявності екосистеми Microsoft — у порівнянні з іншими рішеннями ця система не потребує складних налаштувань для інтеграції з хмарою Azure та корпоративною системою адміністрації Active Directory, тобто надає нативне і більш оптимізоване рішення для засобів та рішень Microsoft [24].

Зважаючи на те, що Microsoft Sentinel переважно використовується у хмарному середовищі, воно використовує передові рішення у сфері ШІ для кореляції даних, виявлення аномалій та рекомендацій щодо усунення недоліків [25]. Ця SIEM-система має змогу аналізувати загальний стан захищеності інфраструктури та створювати звіти з оцінкою стану за певними критеріями, що може бути необхідним для відповідності

безпековим стандартам. Це дозволяє використовувати хмарне середовище для певних елементів критичної інфраструктури, надаючи такі переваги, як постійна доступність та фізична захищеність.

Варто зазначити, що залежність від екосистеми може бути недоліком цієї SIEM-системи. Хоч Sentinel має доповнення-інтеграції її іншими безпековими рішеннями, він менш ефективний у гетерогенних середовищах, де використовуються інші операційні системи та рішення сторонніх виробників.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Кількість загроз у кіберпросторі постійно зростає, і об’єкти критичної інфраструктури та інші організації потребують захисту. SIEM-системи є ключовим інструментом операційного центру безпеки (SOC).

SIEM дозволяють стежити за усією інформаційною інфраструктурою загалом і знаходити залежності між подіями у системах швидше і надійніше. У випадку кіберінцидентів оперативність реагування є ключовим аспектом забезпечення активного кіберзахисту.

Сучасні рішення дозволяють автоматизувати частину процесів з виявлення та реагування на події безпекового характеру, дозволяють брати під контроль гібридні типи інфраструктури, які можуть включати хмарні середовища, системи віртуалізації та контейнеризації, робочі станції та інші корпоративні пристрої.

Враховуючи це, передові SIEM-системи надають змогу організаціям як розгортати свої рішення на власних потужностях, так і орендувати відповідні ресурси, надаючи послугу Software-as-a-Service.

Наявність великої кількості інтеграцій з різноманітними пакетами ПЗ та системами дозволяє SIEM стежити за відповідністю наявного стану кіберзахисту інформаційної інфраструктури організації певним міжнародним стандартам, як то ISO 27001, GDPR чи PCI DSS.

Передові досягнення у сферах машинного навчання та штучного інтелекту використовуються у SIEM для виявлення аномалій у поведінці систем та користувачів, а також для пріоритизації виявлених вразливостей та пропонування кроків щодо покращення стану кіберзахисту.

Як пропрієтарні, так і вільні рішення працюють у спілці з іншими сучасними системами, як то SOAR чи EDR/XDR, які підвищують ефективність SIEM-систем та, як наслідок, операційних центрів безпеки, тому, на думку авторів, відповідні технології заслуговують на подальше дослідження.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *The number of cyberattacks during the war tripled.* (2022). State Service for Special Communications and Information Protection of Ukraine. https://cip.gov.ua/ua/news/kilkist-kiberatak-pid-chas-viini-zrosla-vtrichi
2. Leung, B. K. (2021). *Security Information and Event Management (SIEM) Evaluation Report.* ScholarWorks. https://scholarworks.calstate.edu/downloads/41687p49q
3. González-Granadillo, G., González-Zarzosa, S., Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors, 21(14).* https://doi.org/10.3390/s21144759

4. Muhammad, S., et al. (2023). Effective Security Monitoring Using Efficient SIEM Architecture. *Human-centric Computing and Information Sciences, 13.* https://doi.org/10.22967/HCIS.2023.13.017
5. *Magic Quadrant for Security Information and Event Management.* (n. d.). Gartner. https://www.gartner.com/doc/reprints?id=1-2AHCXAHG&ct=220701
6. *Guide for Security-Focused Configuration Management of Information Systems.* (2021). NIST. https://doi.org/10.6028/NIST.SP.800-128
7. *What is SIEM. Security Information and Event Management Tools.* (n. d.). Imperva. https://www.imperva.com/learn/application-security/siem/
8. *SOAR and SIEM in 2023: Key Trands and New Changes.* (2023). Security Intelligence. https://securityintelligence.com/articles/soar-and-siem-in-2023-key-trends-and-new-changes/
9. *2022 Gartner® Magic Quadrant™ for SIEM.* (n. d.). Splunk. https://www.splunk.com/en_us/form/gartner-siem-magic-quadrant.html
10. *Splunk Enterprise Security.* (n. d.). Splunk. https://www.splunk.com/en_us/products/enterprise-security.html
11. *Splunk Cloud Platform.* (n. d.). Splunk. https://www.splunk.com/en_us/products/splunk-cloud-platform.html
12. *Elastic Security Solution.* (n. d.). Elastic. https://www.elastic.co/security/
13. *SIEM & Security Analytics | Elastic Security | Elastic SIEM.* (n. d.). Elastic. https://www.elastic.co/security/siem/
14. *Visual event analyzer | Elastic Security Solution [8.12] | Elastic.* (n. d.). Elastic — The Search AI Company | Elastic. https://www.elastic.co/guide/en/security/current/visual-event-analyzer.html
15. *IBM Security QRadar.* (n. d.) https://www.ibm.com/qradar/
16. *What is the MITRE ATT&CK Framework? | IBM.* (n. d.). https://www.ibm.com/topics/mitre-attack/
17. *IBM QRadar SIEM Solution Brief.* (n. d.). https://www.ibm.com/downloads/cas/RLXJNX2G
18. *Overview | Wazuh.* (n. d.). https://wazuh.com/platform/overview/
19. *Wazuh – The Open Source Security Platform. Unified XDR and SIEM protection for endpoints and cloud workloads.* (n. d.). https://github.com/wazuh/wazuh?tab=readme-ov-file#wazuh
20. *Regulatory compliance – Wazuh documentation.* (n. d.). https://documentation.wazuh.com/current/compliance/index.html
21. *How SCA works – Security Configuration Assessment.* (n. d.). https://documentation.wazuh.com/current/user-manual/capabilities/sec-config-assessment/how-it-works.html
22. *Wazuh License.* (n. d.). https://github.com/wazuh/wazuh/blob/master/LICENSE
23. *Microsoft Sentinel – хмарне SEIM-рішення.* (n. d.). https://www.microsoft.com/uk-ua/security/business/siem-and-xdr/microsoft-sentinel/
24. *Moving to Next-Gen SIEM with Microsoft Sentinel.* (n. d.). https://www.microsoft.com/insidetrack/blog/moving-to-next-generation-siem-at-microsoft-with-microsoft-azure-sentinel/
25. *What is Microsoft Sentinel?* (n. d.). https://learn.microsoft.com/uk-ua/azure/sentinel/overview/
26. Smirnov, O., et al. (2023). Simulation of the cloud IoT-based monitoring system for critical infrastructures. In: *CEUR Workshop Proceedings, vol. 3530,* 256–265.
27. Smirnov, O., et al. (2022). Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine. In: *CEUR Workshop Proceedings, vol. 3187,* 1–12.
28. Smirnov, O., et al. (2023). Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm. *Intelligent Communication Technologies and Virtual Mobile Networks, 131,* 21–34.
29. Smirnov O. A., et al. (2020). Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources. *Journal of Theoretical and Applied Information Technology, 98(21),* 3334–3346.
30. Smirnov O. A., et al. (2020). Research of cloud technologies as services. *Cybersecurity: Education, Science, Technology, 3(7),* 43–62.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

**Tetiana Smirnova**
PhD, Associate Professor of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-6896-0612
*sm.tetyana.gmail.com*

**Liliia Konstantynova**
Lecturer of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0002-3305-2427
*liliyashel1976@gmail.com*

**Oksana Konoplitska-Slobodeniuk**
Lecturer of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-9981-5194
*ksuha80@gmail.com*

**Yan Kozlov**
Student of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0009-0006-1617-4074
*kozlov.yan1@gmail.com*

**Oksana Kravchuk**
HR Department Inspector
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0009-0008-8453-0557
*vov-14@i.ua*

**Nataliia Kozirova**
Assistant of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0009-0005-8753-5132
*natalidonchenko23@gmail.com*

**Oleksii Smirnov**
Doctor of Technical Sciences, Professor,
Head of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-9543-874X
*dr.smirnovoa@gmail.com*

# STUDY OF THE CURRENT STATE OF SIEM SYSTEMS

**Abstract.** In this work, a study of SIEM systems, the relevance of which has grown significantly during the full-scale invasion of Russia into Ukraine, has been carried out. The task of finding the most optimal solutions was solved according to the following criteria: ease of use, ability to integrate with other protection solutions, pricing policy and features. For this purpose, the work considered a general description of the structure and principle of operation of the SIEM system, determined the capabilities and features of modern SIEM systems, conducted a study of the following software (software): Splunk Enterprise Security (Splunk), Elastic Security, IBM QRadar SIEM, Wazuh SIEM, Microsoft Sentinel. As a result of the research, the following was revealed: modern SIEM solutions allow automating part of the processes of detection and response to security events, allow to take control of hybrid types of infrastructure, which may include cloud environments, virtualization and containerization systems, workstations and other corporate devices. They are implemented both in the form of deployment of their solutions at their own facilities, and in the form of renting relevant resources, providing a Software-as-a-Service service. At the same time, the presence of a large number of integrations with various software packages and systems allows SIEM

to monitor the compliance of the current state of cyber protection of the organization's information infrastructure with certain international standards, such as ISO 27001, GDPR or PCI DSS. It was determined that modern SIEMs use advances in machine learning and artificial intelligence to detect anomalies in system and user behavior, as well as to prioritize identified vulnerabilities and suggest steps to improve the state of cyber defense. The considered solutions work in conjunction with other modern systems, such as SOAR or EDR/XDR, which increases the efficiency of SIEM systems and, as a result, security operation centers, therefore, according to the authors, the corresponding technologies deserve further research.

**Keywords:** SIEM; security information and event management; cloud platforms; critical infrastructure; cyber security; informational security.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *The number of cyberattacks during the war tripled.* (2022). State Service for Special Communications and Information Protection of Ukraine. https://cip.gov.ua/ua/news/kilkist-kiberatak-pid-chas-viini-zrosla-vtrichi
2. Leung, B. K. (2021). *Security Information and Event Management (SIEM) Evaluation Report.* ScholarWorks. https://scholarworks.calstate.edu/downloads/41687p49q
3. González-Granadillo, G., González-Zarzosa, S., Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors, 21(14).* https://doi.org/10.3390/s21144759
4. Muhammad, S., et al. (2023). Effective Security Monitoring Using Efficient SIEM Architecture. *Human-centric Computing and Information Sciences, 13.* https://doi.org/10.22967/HCIS.2023.13.017
5. *Magic Quadrant for Security Information and Event Management.* (n. d.). Gartner. https://www.gartner.com/doc/reprints?id=1-2AHCXAHG&ct=220701
6. *Guide for Security-Focused Configuration Management of Information Systems.* (2021). NIST. https://doi.org/10.6028/NIST.SP.800-128
7. *What is SIEM. Security Information and Event Management Tools.* (n. d.). Imperva. https://www.imperva.com/learn/application-security/siem/
8. *SOAR and SIEM in 2023: Key Trands and New Changes.* (2023). Security Intelligence. https://securityintelligence.com/articles/soar-and-siem-in-2023-key-trends-and-new-changes/
9. *2022 Gartner® Magic Quadrant™ for SIEM.* (n. d.). Splunk. https://www.splunk.com/en_us/form/gartner-siem-magic-quadrant.html
10. *Splunk Enterprise Security.* (n. d.). Splunk. https://www.splunk.com/en_us/products/enterprise-security.html
11. *Splunk Cloud Platform.* (n. d.). Splunk. https://www.splunk.com/en_us/products/splunk-cloud-platform.html
12. *Elastic Security Solution.* (n. d.). Elastic. https://www.elastic.co/security/
13. *SIEM & Security Analytics | Elastic Security | Elastic SIEM.* (n. d.). Elastic. https://www.elastic.co/security/siem/
14. *Visual event analyzer | Elastic Security Solution [8.12] | Elastic.* (n. d.). Elastic — The Search AI Company | Elastic. https://www.elastic.co/guide/en/security/current/visual-event-analyzer.html
15. *IBM Security QRadar.* (n. d.) https://www.ibm.com/qradar/
16. *What is the MITRE ATT&CK Framework? | IBM.* (n. d.). https://www.ibm.com/topics/mitre-attack/
17. *IBM QRadar SIEM Solution Brief.* (n. d.). https://www.ibm.com/downloads/cas/RLXJNX2G
18. *Overview | Wazuh.* (n. d.). https://wazuh.com/platform/overview/
19. *Wazuh – The Open Source Security Platform. Unified XDR and SIEM protection for endpoints and cloud workloads.* (n. d.). https://github.com/wazuh/wazuh?tab=readme-ov-file#wazuh
20. *Regulatory compliance – Wazuh documentation.* (n. d.). https://documentation.wazuh.com/current/compliance/index.html
21. *How SCA works – Security Configuration Assessment.* (n. d.). https://documentation.wazuh.com/current/user-manual/capabilities/sec-config-assessment/how-it-works.html
22. *Wazuh License.* (n. d.). https://github.com/wazuh/wazuh/blob/master/LICENSE

23. *Microsoft Sentinel – хмарне SEIM-рішення.* (n. d.). https://www.microsoft.com/uk-ua/security/business/siem-and-xdr/microsoft-sentinel/
24. *Moving to Next-Gen SIEM with Microsoft Sentinel.* (n. d.). https://www.microsoft.com/insidetrack/blog/moving-to-next-generation-siem-at-microsoft-with-microsoft-azure-sentinel/
25. *What is Microsoft Sentinel?* (n. d.). https://learn.microsoft.com/uk-ua/azure/sentinel/overview/
26. Smirnov, O., et al. (2023). Simulation of the cloud IoT-based monitoring system for critical infrastructures. In: *CEUR Workshop Proceedings, vol. 3530,* 256–265.
27. Smirnov, O., et al. (2022). Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine. In: *CEUR Workshop Proceedings, vol. 3187,* 1–12.
28. Smirnov, O., et al. (2023). Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm. *Intelligent Communication Technologies and Virtual Mobile Networks, 131,* 21–34.
29. Smirnov O. A., et al. (2020). Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources. *Journal of Theoretical and Applied Information Technology, 98(21),* 3334–3346.
30. Smirnov O. A., et al. (2020). Research of cloud technologies as services. *Cybersecurity: Education, Science, Technology, 3(7),* 43–62.