УДК 341.4
DOI 10.36919/3041-1149(Print).8.2025.56-62

О. К. Саморай,
викладач кафедри кібербезпеки,
ПВНЗ «Європейський університет»
email: oleg.samorai@gmail.com
ORCID 0009-0000-3384-155X;
О. О. Семенюк,
кандидат юридичних наук, доцент,
доцент кафедри права,
ПВНЗ «Європейський університет»
email: sashasemenujk@gmail.com
ORCID 0009-0007-9199-6657

ТЕОРЕТИЧНІ Й ПРАКТИЧНІ ПІДХОДИ ДО РОЗУМІННЯ КІБЕРІНЦИДЕНТІВ ТА ЇХНЬОЇ ІДЕНТИФІКАЦІЇ

У статті проаналізовано теоретичні та практичні підходи до розуміння й ідентифікації кіберінцидентів у сучасному інформаційному просторі. Обґрунтовано актуальність досліджуваної проблематики в контексті стрімкого розвитку цифрових технологій та, як наслідок, зростання кількості кіберзагроз.

Метою статті є дослідження теоретичних і практичних підходів до розуміння поняття «кіберінцидент»; з'ясування інструментарію для коректної ідентифікації, класифікації та фіксації кіберінцидентів і подальшого правового реагування на них.

Проведено категоризацію кіберінцидентів (технічні, інциденти безпеки, соціальні та фізичні), а також надано опис багаторівневої архітектури AI-оптимізованої SIEM для зниження кількості хибних спрацювань і пріоритизації подій.

Окремо проаналізовано юридичні вимоги до збору, збереження й незмінності цифрових артефактів, потрібних для правового реагування та закріплення доказової бази в можливих кримінальних провадженнях. Запропоновано рекомендації з уніфікації термінології та вдосконалення процедур класифікації й реагування на кіберінциденти, що сприятимуть підвищенню ефективності державних і корпоративних систем кібербезпеки.

Ключові слова: *кіберінцидент, кіберзагроза, кіберпростір, національна безпека, SIEM-системи, кібербезпека, приватна інформація.*

Постановка проблеми та її актуальність. Сучасний світ характеризується стрімким розвитком цифрових технологій, що призводить до зростання ризиків, пов'язаних із кіберзагрозами. Такі загрози мають глобальний характер і можуть спричинити серйозні негативні наслідки як для окремих осіб, так і для національної безпеки, економічної стабільності та захисту прав і свобод людини та громадянина в кіберпросторі.

Кіберінциденти, які є результатом таких загроз, містять у собі не лише атаки на IT-системи, але й порушення безпеки персональних даних, фінансових інститутів, критичної інфраструктури. Виявлення, реагування та своєчасне усунення кіберінцидентів є важливою складовою забезпечення безпеки держави й суспільства. У цьому зв'язку вагомим є розуміння того факту, що ефективне реагування на кіберінциденти потребує скоординованих зусиль державних і бізнес-структур, а також окремих громадян для зменшення ризиків і мінімізації наслідків таких інцидентів. Актуальність проблеми зумовлена також рядом інших чинників. Зокрема, це глобалізація кіберзагроз, яка ускладнює боротьбу з ними на міжнародному рівні, оскільки правові та технічні норми часто не узгоджуються на міждержавному рівні. Стрімкий розвиток технологій, розширення використання інтернету речей (IoT) та штучного інтелекту, зростає й рівень вразливості різних секторів економіки, що, безумовно, створює нові можливості для кіберінцидентів. На жаль,

варто констатувати, що на сьогодні в Україні, як і в інших країнах світу, існує нагальна потреба в удосконаленні законодавства у сфері кібербезпеки, адже сучасні законодавчі ініціативи часто не відповідають швидкозмінним умовам кіберзагроз.

Аналіз останніх досліджень та публікацій. Проблемні питання, пов'язані з дослідженням кіберінцидентів, активно розглядалися здебільшого в контексті національної безпеки. У роботах таких авторів, як О. В. Скрипник, М. П. Баранов, В. І. Цимбалюк та інших, акцентується увага на потребі в побудові ефективної системи державного реагування на кіберінциденти, розробки національних стандартів кіберзахисту, а також удосконалення законодавчої бази. Зокрема, аналізуються проблеми ідентифікації кіберінцидентів та особливості взаємодії між суб'єктами кіберзахисту в Україні. Зарубіжні автори, зокрема R. Kissel, B. Schneier та G. Ollmann, розглядають кіберінциденти в контексті управління інформаційною безпекою, моделювання загроз та інцидент-менеджменту.

Метою статті є дослідження теоретичних і практичних підходів до розуміння поняття «кіберінцидент»; з'ясування інструментарію для коректної ідентифікації, класифікації та фіксації кіберінцидентів для подальшого правового реагування на них.

Виклад основного матеріалу дослідження. У науковій літературі термін «кіберінцидент» розуміється по-різному, залежно від контексту застосування та сфери наукового пошуку. Так, під *кіберінцидентом* розуміють подію або серію подій у кіберпросторі, які можуть призвести до порушення конфіденційності, цілісності та доступності інформації й інформаційних систем. Це поняття може охоплювати як умисні, так і ненавмисні події, що негативно впливають на роботу комп'ютерних мереж і систем [1]. *Кіберінцидентом* вважають подію, яка негативно впливає на інформаційні системи організації, як-от витік даних або зловмисна атака [2]. *Кіберінцидент* як спроба використання недосконалості системи безпеки з метою отримання інформації або нанесення шкоди системі [3].

Наведені визначення досліджуваного поняття вказують на негативний вплив на інформаційні системи, проте кожне з них акцентує увагу на різних аспектах подій. В одному випадку кіберінцидент може бути результатом серії подій у кіберпросторі, які порушують конфіденційність, цілісність і доступність інформації. В іншому – це витік даних чи навмисні атаки, що безпосередньо загрожують безпеці та функціональності цих систем. Третє розуміння акцентує увагу на використанні вразливостей у системах безпеки з метою отримання конфіденційної інформації або заподіяння шкоди, через активне використання недосконалості системи для здійснення атаки.

Однак усі ці визначення об'єднує спільний фокус на порушенні роботи інформаційних систем, яке може мати серйозні наслідки для їхнього функціонування незалежно від того, чи є такі дії умисними або необережними, або ж ідеться про використання недосконалості системи для досягнення злочинної мети [4, с. 209].

Кіберінциденти можуть мати негативні наслідки для держави, підприємств, установ, організацій незалежно від форми власності, а також окремих користувачів. Вони впливають на конфіденційність, цілісність і доступність інформації, що може призвести до фінансових втрат, репутаційних ризиків і навіть зупинки роботи систем управління інформацією.

У цьому контексті кіберінциденти можна диференціювати на чотири категорії:

Технічні інциденти – пов'язані з апаратними та програмними збоями, які можуть призвести до порушення роботи інформаційних систем. Зазвичай вони виникають через: несправність серверів, жорстких дисків, мережевого обладнання або інших критично важливих компонентів системи; уразливості та недосконалості програмного коду; технічних конфліктів між програмним забезпеченням; збоях під час оновлення або проблемах із несумісністю програмного забезпечення; відмови маршрутизаторів, перевантаження каналів зв'язку; низькою якістю надання послуг інтернет-провайдерами; DDoS-атак – масового надсилання запитів з метою перевантаження ресурсів, що призводить до часткової або повної втрати доступу до інформаційних систем.

Інциденти безпеки – пов'язані із загрозами інформаційній безпеці та можуть спричинити витік або викрадення конфіденційних даних. Випадками таких інцидентів є: злом користувацьких акаунтів, підбір паролів або використання вразливостей для проникнення в корпоративні або державні системи; копіювання, публікація чи передача критично важливої інформації;

розповсюдження вірусів, троянів, програми-вимагачів, які можуть зашифрувати дані або отримати контроль над системою.

Соціальні інциденти – вчиняються через психологічний вплив на користувачів з метою доступу до конфіденційної інформації. До таких інцидентів належать: розсилка підроблених електронних листів або повідомлень, що імітують офіційні джерела з метою викрадення облікових даних; маніпуляція користувачами для отримання доступу до систем або даних, наприклад через нав'язливі телефонні дзвінки, шахрайські запити або обман у соцмережах.

Фізичні інциденти – це події, які спричиняють фізичне пошкодження або втрату інформаційних систем, мережевого обладнання чи носіїв даних. Найпоширенішими випадками фізичних інцидентів є: викрадення або повне знищення апаратного забезпечення – крадіжка ноутбуків, серверів або накопичувачів даних; руйнівна дія природних явищ – повені, пожежі, землетруси або інші катаклізми, які можуть пошкодити серверні приміщення або центри обробки даних; збої в системах кондиціонування або живлення, які можуть призвести до перегріву серверів і, як наслідок, вихід обладнання з ладу або втрату даних.

З огляду на різноманітність і зростаючу складність кіберінцидентів, що можуть мати технічну, інформаційну, соціальну або фізичну природу, особливої актуальності набуває впровадження ефективних інструментів для їхнього виявлення, аналізу, реагування, а в кінцевому випадку й правової оцінки. Одним із таких ключових інструментів у сфері кібербезпеки є SIEM (Security Information and Event Management) – система управління інформацією про безпеку та подіями, яка збирає дані про події безпеки з додатків, мережі, кінцевих точок і хмарних середовищ, а потім використовує їх для моніторингу безпеки, виявлення загроз і реагування на них, а також і оцінки ризиків [5, с. 201].

У сучасних умовах зростаючого обсягу кіберінцидентів традиційні SIEM-системи дедалі частіше демонструють обмежену здатність своєчасно виявляти кіберзагрози без значної кількості хибних спрацювань. Так, дослідження, проведене University of Oxford, виявило, що деякі системи виявлення вторгнень можуть генерувати до 99 % хибнопозитивних сповіщень, що призводить до перевантаження аналітиків безпеки та зниження ефективності реагування на реальні загрози [6]. Проте, за даними компанії Alberta Health Services, спостерігається деяке зниження кількості хибнопозитивних сповіщень на 90 % після переходу на хмарну SIEM-платформу Securonix з використанням машинного навчання та штучного інтелекту [7]. Вочевидь результати проведених досліджень обумовлюють потребу в обов'язковому переході на SIEM-системи з використанням штучного інтелекту та машинного навчання для зменшення кількості хибнопозитивних сповіщень і підвищення ефективності роботи центрів операцій безпеки.

Використання машинного навчання й штучного інтелекту в контексті SIEM систем дає змогу підвищити їх ефективність. Замість фіксованих правил ШІ-модулі, які навчені на реальних даних, автоматично корелюють різні події за допомогою моделей класифікації, виявляють аномалії та пріоритизують інциденти за ризиком. Такі підходи показують високу ефективність у виявленні нетипової поведінки й зменшенні навантаження на фахівців з кіберзахисту.

У практичному застосуванні загальна архітектура ШІ-оптимізованої SIEM охоплює п'ять логічних шарів: це шар збору даних (логування, мережевий трафік, DNS – аналіз доменних імен, EDR – дослідження серверних запитів / відповідей); функціональне сховище для попереднього обчислення ознак у реальному часі; офлайн-середовище для поетапного тренування й валідації моделей; двигун логічного виводу для детекції та кореляції в режимі реального часу; шар візуалізації й інтеграції зі SOAR (платформа або набір інструментів, що дає змогу автоматизувати процеси виявлення, аналізу та реагування на кіберінциденти) [8]. Така схема дає нагоду розділити роботу SIEM-системи на два етапи: на оффлан (тренування) та онлайн (детекція). Що, безумовно, забезпечує швидкість і надійність роботи системи.

Наведена вище багаторівнева архітектура SIEM дає змогу впровадити досить широкий спектр методів інтелектуального аналізу даних для виявлення кіберзагроз. Одним із найпоширеніших підходів є *детекція аномалій із використанням автоенкодерів і кластеризації.* Цей патерн є одним із ключових підходів у виявленні аномалій мережевого трафіку, особливо під час виявлення кіберзагроз і моніторингу систем. Автоенкодери навчаються відтворювати «здоровий» мережевий

трафік, а події з похибкою відновлення вищевстановленого порога вважаються аномальними. Застосування поетапного навчання дає змогу оновлювати моделі без зупинки роботи системи та виявляти нові відхилення в режимі реального часу.

Іншим поширеним патерном аналізу даних для виявлення кіберзагроз є *графова кореляція подій*. Цей підхід базується на представленні ІТ-інфраструктури та її активностей як *графа*, де: *вузли* (nodes) відповідають об'єктам системи: користувачам, пристроям (хостам), процесам, обліковим записам, сервісам та ін.; *ребра* (edges) репрезентують взаємодії між цими об'єктами: наприклад, аутентифікацію, передачу файлів, мережеві з'єднання, запуск процесів чи зміну прав доступу користувача. За допомогою методів прогнозування зв'язку (Link prediction) і баєсових мереж (Bayesian networks) формується єдина картина кіберінциденту.

Завдяки такій графовій структурі система не просто реагує на окремі події, а будує причинно-наслідкові зв'язки між ними. Це насамперед дає змогу фахівцям з кібербезпеки об'єднувати серію передусім незначних або розрізнених подій у єдину загрозу, а також виявляти багатоетапні атаки (multi-stage attacks), зокрема як-от APT (Advanced Persistent Threat), які здійснюються повільно й приховано, використовуючи легітимні процеси.

У сучасних системах кіберзахисту обсяг згенерованих кіберінцидентів може сягати десятків тисяч на день, що робить мануальну обробку всіх інцидентів практично неможливою та вимагає великої витрати людських ресурсів. Для ефективного використання ресурсів аналітиків безпеки (SOC) застосовується автоматизована система сортування та пріоритизації подій за допомогою моделей машинного навчання (ML).

Моделі ML отримують на вхід набір ознак, які описують кожну подію або інцидент у контексті: часу доби – аномальні дії в нетиповий час (наприклад, о 3:00 ночі) мають вищу підозрілість; геолокації IP-адреси – підозріла активність із нетипових країн чи регіонів; історичного ризикового профілю користувача / хоста – чи були раніше інциденти, пов'язані з цим об'єктом? Як часто фіксується підозріла активність?; типу подій – підозрілий вхід у систему, запуск скрипта, зміна привілеїв; контексту взаємодії – які інші об'єкти були залучені до інциденту [9].

Після завершення процесу аналізу кіберінцидентів аналітики SOC дають зворотний зв'язок, уточнюючи чи була подія реальною загрозою. Водночас у разі виявлення кіберзагроз зібрана аналітична інформація може містити ознаки кримінальних правопорушень, що є підставою звернення до правоохоронних органів, а також є потенційно допустимим доказом у кримінальному провадженні за умови належного документування та зберігання.

У разі виявлення кіберінциденту, який містить ознаки кримінального правопорушення, зібрані цифрові артефакти можуть бути додані до офіційного звернення в правоохоронні органи (Національну поліцію, СБУ). До таких артефактів можуть належати: журнали подій (логи) з точним часом; IP-адреси серверів, з яких вчинялися атаки; дампи мережевого трафіку або знімки систем; матеріали результатів внутрішнього розслідування інциденту.

Проте для того щоб дані, зібрані SIEM, могли бути використані не лише для виявлення й реагування на кіберінциденти, а й як юридично допустимі докази, ці системи повинні відповідати ряду критичних вимог – як з боку інформаційної безпеки, так і з боку процесуального права.

По-перше, SIEM-система повинна забезпечувати безперервний збір і збереження журналів подій, зокрема: точний час події (timestamp), з урахуванням часових поясів і синхронізації; ідентифікатор користувача, процесу або сервісу, що ініціював шкідливу дію; IP-адресу джерела / отримувача, MAC-адресу (за можливості); тип дії (аутентифікація, доступ до файлів, мережеві з'єднання, виконання команд та ін.). Адже неперервність і повнота логів дасть змогу побудувати хронологічну картину інциденту, яка матиме доказову цінність досудового розслідування, судового розгляду або під час проведення експертиз.

По-друге, з метою уникнення можливих звинувачень у фальсифікації матеріалів документування кіберінцидентів важливо забезпечити технічні механізми, що гарантують незмінність зібраної інформації. Зокрема, обов'язковим є: застосування криптографічних хеш-функцій (SHA-256 і вище) до файлів, в яких містяться логи; наявність електронних підписів суб'єктів, відповідальних за роботу систем або їхніх адміністраторів; створення та належне зберігання контрольних копій логів у незмінному (read-only) сховищі; журналювання доступу безпосередньо до системи логування для розуміння, хто, коли і з якою метою переглядав чи змінював дані.

Відповідно до змісту законів України «Про захист інформації в інформаційно-телекомунікаційних системах» [10] та «Про захист персональних даних» [11] аналітичні системи обов'язково повинні функціонувати в межах чітко визначених внутрішніх регламентів, які мають передбачати: чіткі терміни зберігання даних (наприклад, не менше 1 року згідно з окремими регуляціями НБУ, КСЗІ та ін.); диференціацію рівнів доступу до журналів подій (на підставі ролей або повноважень); перманентні перевірки стану збереженості, цілісності та повноти журналів; затвердження відповідальних співробітників за технічну й організаційну безпеку обробки кіберінцидентів.

Висновки. Викладене вище дає змогу зробити такі узагальнення:

1. Проаналізовані підходи до розуміння поняття «кіберінцидент» демонструють розбіжності в його розумінні: одні автори додають до нього всі події, що порушують конфіденційність, цілісність або доступність інформаційних систем, інші – тільки навмисні атаки чи зловмисні дії. Така варіативність ускладнює координацію дій між суб'єктами кібербезпеки та створює правові прогалини в кваліфікації інцидентів.

Запропонована авторами чотирирівнева класифікація (технічні, інциденти безпеки, соціальні, фізичні) забезпечує цілісний огляд можливих загроз і полегшує вибір адекватних методів виявлення та реагування на кожен тип події.

2. Сучасні SIEM-системи досить часто мають значний відсоток хибних спрацювань. Впровадження машинного навчання та штучного інтелекту дає змогу зменшити їх кількість до 90 % та підвищити точність детекції аномалій за допомогою моделей автоенкодерів, кластеризації та графової кореляції.

3. Під час виявлення кіберінциденту, який містить ознаки кримінального правопорушення, зібрані матеріали його дослідження можуть бути додані до офіційного звернення в правоохоронні органи (Національну поліцію, СБУ). До таких артефактів можуть належати: журнали подій (логи) з точним часом; IP-адреси серверів, з яких вчинялися атаки; дампи мережевого трафіку або знімки систем; матеріали результатів внутрішнього розслідування інциденту.

Проте для того щоб дані, зібрані SIEM, могли бути використані не лише для виявлення й реагування на кіберінциденти, а й як юридично допустимі докази, ці системи повинні відповідати ряду критичних вимог – як з боку інформаційної безпеки, так і з боку процесуального права.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пахольченко Д. О., Тимошенко Г. С., Фартушний В. В. Методика визначення категорії (рівня) критичності кіберінциденту / кібератаки. *ResearchGate*. 2023. URL : https://www.researchgate.net/publication/371138727

2. VPN Unlimited. Що таке кіберінцидент? URL : https://www.vpnunlimited.com/ua/help/cybersecurity/cyber-incident

3. Кіберінциденти та їх класифікація / Луцький національний технічний університет. URL : https://e-tk.lntu.edu.ua/mod/resource/view.php?id=13440

4. Семенюк О. О. До питання правового розуміння поняття «гіберінцидент». *Розвиток юридичної науки України в умовах воєнного стану. Юридична наука: проблеми та шляхи їх вирішення* : збірник матеріалів І Міжнародної науково-практичної конференції, м. Київ, 6 березня 2025 року. Київ : Приватний вищий навчальний заклад «Європейський університет», 2025. С. 208–210.

5. Аналіз відкритих систем виявлення вторгнень / Терейковський І. А., Корченко А. О., Паращук Т. І., Педченко Є. М. *Ukrainian Scientific Journal of Information Security*. 2018. Т. 24, № 3. С. 201–216.

6. Alahmadi A., Onarlioglu K., Polychronakis M. Intrusion Detection for the Modern Era: The Performance of Signature, Anomaly, and Specification-based Approaches / Proceedings of the 31st USENIX Security Symposium. 2022. URL : https://www.usenix.org/system/files/sec22summer_alahmadi.pdf

7. Securonix. Alberta Health Services Reduces False Positives with Securonix / Securonix Case Study. 2022. URL : https://www.securonix.com/wp-content/uploads/2022/09/Alberta-Health-Services-Reduces-False-Positives-with-Securonix.pdf

8. Lanz J. The Updated NIST Cybersecurity Framework. *The CPA Journal*. 2024. Vol. 94, No. 5/6. P. 70–72.

9. Google Cloud. Chronicle Security Operations. URL : https://cloud.google.com/chronicle

10. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL : https://zakon.rada.gov.ua/laws/show/80/94-вр

11. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL : https://zakon.rada.gov.ua/laws/show/2297-17

REFERENCES

1. Pakholchenko, D. O., Tymoshenko, H. S., Fartushnyi, V. V. (2023). Metodyka vyznachennya katehoriyi (rivnya) krytychnosti kiberintsydentu / kiberataky [Methodology for determining the category (level) of criticality of a cyber incident/cyber attack]. ResearchGate. URL : https://www.researchgate.net/publication/371138727 [in Ukrainian].

2. VPN Unlimited. Shcho take kiberintsydent? [What is a cyber incident?]. URL : https://www.vpnunlimited.com/ua/help/cybersecurity/cyber-incident [in Ukrainian].

3. Lutsk National Technical University. Kiberintsydenty ta yikh klasyfikatsiya [Cyber incidents and their classification]. URL : https://e-tk.lntu.edu.ua/mod/resource/view.php?id=13440 [in Ukrainian].

4. Semeniuk, O. O. (2025). Do pytannya pravovoho rozuminnya ponyattya «Kiberintsydent» [On the issue of legal understanding of the concept of "Cyber Incident"]. *Development of legal science of Ukraine under martial law. Legal science: problems and ways to solve them* : collection of materials of the I International Scientific and Practical Conference, Kyiv, March 6, 2025. Kyiv : Private higher educational institution "European University", 208–210 [in Ukrainian].

5. Analiz vidkrytykh system vyyavlennya vtorhnen′ [Analysis of open intrusion detection systems] / Tereikovskyi, I. A., Korchenko, A. O., Parashchuk, T. I., Pedchenko, Ye. M. *Ukrainian Scientific Journal of Information Security*. 2018. 24 (3), 201–216 [in Ukrainian].

6. Alahmadi, A., Onarlioglu, K., Polychronakis, M. (2022). Intrusion Detection for the Modern Era: The Performance of Signature, Anomaly, and Specification-based Approaches / Proceedings of the 31st USENIX Security Symposium. URL : https://www.usenix.org/system/files/sec22summer_alahmadi.pdf

7. Securonix. (2022). Alberta Health Services Reduces False Positives with Securonix. Securonix Case Study. URL : https://www.securonix.com/wp-content/uploads/2022/09/Alberta-Health-Services-Reduces-False-Positives-with-Securonix.pdf

8. Lanz, J. (2024). The Updated NIST Cybersecurity Framework. *The CPA Journal.* 94 (5/6), 70–72.

9. Google Cloud. Chronicle Security Operations. URL : https://cloud.google.com/chronicle [in Ukrainian].

10. Law of Ukraine on protection of information in information and telecommunication systems dated July 5, 1994 No. 80/94-VR. URL : https://zakon.rada.gov.ua/laws/show/80/94-вр [in Ukrainian].

11. Law of Ukraine on personal data protection dated June 1, 2010 No. 2297-VI. URL : https://zakon.rada.gov.ua/laws/show/2297-17 [in Ukrainian].

O. K. Samorai, O. O. Semenuk. THEORETICAL AND PRACTICAL APPROACHES TO UNDERSTANDING CYBER INCIDENTS AND THEIR IDENTIFICATION

The article analyzes theoretical and practical approaches to understanding and identifying cyber incidents in the modern information space. The relevance of the research topic is substantiated in the context of the rapid development of digital technologies and the consequent increase in the number of cyber threats.

The purpose of the article is to study theoretical and practical approaches to understanding the concept of "cyber incident"; clarifying the tools for correct identification, classification, and recording of cyber incidents and subsequent legal response to them.

A categorization of cyber incidents (technical, security incidents, social, and physical) is provided, as well as a description of the multi-level architecture of AI-optimized SIEM to reduce the number of false positives and prioritize events.

Additionally, the legal requirements for collecting, storing, and maintaining the immutability of digital artifacts necessary for legal response and securing evidence in possible criminal proceedings are analyzed. Recommendations for unifying terminology and improving procedures for classification and response to cyber incidents are proposed, which will enhance the effectiveness of state and corporate cybersecurity systems.

Key words: *cyber incident, cyber threat, cyberspace, national security, SIEM systems, cybersecurity, private information.*