УДК 004.056–047.64
DOI 10.31494/2412-9208-2021-1-2-177-186

SECURITY OPERATIONS CENTER AS A SERVICE BASED ON SIEM

ОПЕРАЦІЙНИЙ ЦЕНТР БЕЗПЕКИ ЯК ПОСЛУГА НА ОСНОВІ SIEM

Vasyl BOLILYI,
PhD in Physical and Mathematical Sciences, Associate Professor

Василь БОЛІЛИЙ,
кандидат фізико-математичних наук, доцент

vasyl.bolilyj@gmail.com
https://orcid.org/0000-0002-1923-1058

Volodymyr Vynnychenko Central Ukrainian State Pedagogical University

✉ 1,Shevchenka st., Kropyvnytskiy, Kirovograd region, 25005

Центральноукраїнський державний педагогічний університет імені Володимира Винниченка

✉ вул. Шевченка, 1, м. Кропивницький, Кіровоградська обл., 25005

Liudmyla SUKHOVIRSKA,
PhD of Pedagogical Sciences, Acting Head of the Department

Людмила СУХОВІРСЬКА,
кандидат педагогічних наук, в.о. завідувача кафедри

suhovirskaya2011@gmail.com
https://orcid.org/0000-0003-0353-9354

Olha LUNHOL,
PhD of Pedagogical Sciences, Senior Lecturer

Ольга ЛУНГОЛ,
кандидат педагогічних наук, старший викладач

lunhol_o_m@ukr.net
https://orcid.org/0000-0001-8128-0072

Donetsk National Medical University

✉ 27,Privokzalna st., Liman, Donetsk region, 84401

Донецький національний медичний університет

✉ вул. Привокзальна, 27, м. Лиман, Донецька обл., 84401

Original manuscript received: June 30, 2021
Revised manuscript accepted: September 15, 2021

ABSTRACT

This study examines the Security Operations Center, which provides detection and analysis of cybersecurity, rapid response, and prevention of cyber attacks. Security Operations Center technologies are used to provide visibility and enable analysts to protect against attacks.

The algorithm of presenting the topic «Security Center» during the teaching of the discipline «Security of programs and data» at the Volodymyr Vynnychenko Central Ukrainian State Pedagogical University is shown, namely the problems of implementation of event monitoring systems «Security information and event management», types of operational centers, methods of building internal operational security centers. Subject competencies are formed in students: to classify, identify and

protect information processing facilities from unauthorized access and computer viruses, to develop individual access control and information protection systems.

The process of implementing Security information and event management systems at the enterprise is shown, the main mechanisms of this system using a hierarchical model, the main tasks of the security operational center, the key parameters of the Security Operations Center (organizational model, performance of functions that go beyond the tasks, level of authority), basic rules of correlation.

The commercial security operations center SOC as a Service is considered, which is designed to help work with a huge amount of information, real-time monitoring and response to attacks.

During the laboratory classes, the students analyzed the companies that provide security operations center services (Information Systems Security Partners, Octave Cybersecurity, Infopulse, Omega Security Service) and studied the factors that affect companies when choosing the type Security Operations Center.

Key words: *Security Operations Center, SEIM-systems, cybersecurity, SOC as a Service.*

У зв'язку з розвитком кібератак, їх масштабом і впливом будь-яким організаціям доводиться приймати важливі рішення про те, як економічно ефективно управляти операціями щодо забезпечення безпеки.

Під час викладання дисципліни «Безпека програм та даних» у Центральноукраїнському державному педагогічному університеті імені Володимира Винниченка (ЦДПУ ім. В. Винниченка) викладачі надають знання щодо сучасних стандартів, підходів, методів та засобів захисту програм та даних. При вивченні дисципліни в здобувачів формуються предметні компетентності: класифікувати, ідентифікувати і захищати засоби обробки інформації від несанкціонованого доступу та комп'ютерних вірусів; захищати інформацію персонального комп'ютера та розроблене програмне забезпечення; розробляти індивідуальні системи управління доступом і захистом інформації.

Розслідуванню інцидентів безпеки присвячені праці науковців М. Федотова, Уоррена Круза, Джея Хейзера, В. Голубева, В. Гавловського, В. Цимбалюка, В. Вехова та інших.

Метою роботи є дослідження методів, моделей та видів побудови операційних центрів безпеки.

Методи та методики дослідження. У науково-педагогічному дослідженні використано теоретичний метод: вивчення інформаційних джерел із проблеми дослідження; синтез, порівняння й узагальнення операційних центрів, методів побудови внутрішніх операційних центрів безпеки. Емпіричні методи: тестування, опитування, анкетування, аналіз результатів, які дозволили узагальнити матеріал щодо сучасних стандартів, підходів, методів та засобів захисту програм та даних.

Виклад основного матеріалу. Під час вивчення теми «Центр забезпечення безпеки» в ЦДПУ ім. В. Винниченка розглядаємо проблеми впровадження систем моніторингу подій, види операційних центрів, методи побудови внутрішніх операційних центрів безпеки.

ICV 2019: 79.31
DOI 10.31494/2412-9208-2021-1-2

Операційний центр безпеки (SOC, Security Operations Center) – команда аналітиків, що за допомогою спеціальних систем та технологій вирішують завдання з безпеки: виявлення та аналіз кібербезпеки, оперативне реагування, запобігання їх виникненню та складання звітності.

Технології SOC – це можливості, які необхідні для забезпечення видимості та надання аналітикам можливості для захисту від атак. Зловмисники, що володіють високою кваліфікацією в області інформаційних технологій і володіють різними методами злому, здатні реалізувати складні атаки на IT-інфраструктуру. Це можуть бути масові атаки (найбільш резонансний приклад – вірусні епідемії WannaCry і NotPetya) або цільові, спрямовані на конкретну компанію або галузь. Для того, щоб вчасно зрозуміти, що зловмисники знаходяться в мережі організації, необхідно збирати дані про події з великої кількості джерел. Чим більше джерел, тим більше шансів деактивувати атаку, але такий обсяг даних призводить до появи декількох проблем: складно одночасно проглядати всі дані про події, що надходять з джерел, кожне з яких має свою форму звітності про подію; події з різних джерел можуть бути зв'язані, тому потрібно поставити їх в правильну послідовність; журнали-аудити періодично видаляють події, які зберігаються там, тому важко відновити дані за довгий період (Згуровський, 2018; Корченко, 2008; Кузнецов, 2018).

Для вирішення цих проблем використовують системи моніторингу подій – Security information and event management (SIEM).

На базі даних, зібраних SIEM – системами, проводиться аналіз поведінки користувача в мережі – User and entity behavior analytics (UEBA).

UEBA – тип процесів у кібербезпеці, який ураховує нормальну поведінку користувача та виявляє аномальну поведінку або випадки відхилення від «нормальних» моделей.

Для того, щоб детектувати події на кінцевих вузлах користувачів і серверах в IT-інфраструктурі, використовується засіб класу Endpoint detection and response (EDR). EDR – це платформа, яка здатна виявляти складні і цільові атаки в системі, сервері, будь-якому комп'ютерному пристрої (кінцеві точки) і швидко на них реагувати. Платформа EDR не просто захищає комп'ютерну систему від шкідників, вона вміє моментально помічати нові загрози високої складності й одночасно проявляти реакцію на ситуацію, що виникла.

Для автоматизації збору та аналізу подій всередині трафіку використовуються засоби класу Network traffic analysis (NTA).

NTA – безперервно аналізують мережеву телеметрію і / або записи потоків. Ця система приймає дані телеметрії від безлічі мережевих пристроїв, таких, як маршрутизатори, комутатори і брандмауери, щоб визначити, як виглядає «нормальна» поведінка цих пристроїв. При виявленні аномального трафіку або нерегулярної мережевої активності ці інструменти попереджають групу безпеки про потенційну загрозу (http://surl.li/amgak).

Комерційні SOC також називаються провайдерами керованого сервісу безпеки (Managed Security Service, MSS).

Gartner визначає MSS як моніторинг або управління функціями IT-безпеки, що надаються через загальні служби з віддалених операційних центрів безпеки, а не через персонал на місці (http://surl.li/amgan).

Центр ринку MSS складається з трьох основних функціональних областей: платформи доставлення (Delivery Platforms) – Saas, хмарні / локально розміщені; технічне обслуговування (Technology Maintenance) – доставлення контенту і підтримка технологій; операції із забезпечення безпеки (Security Operations) – сервіс реагування на інциденти та сканери вразливостей.

Процес упровадження SIEM-систем на підприємство складається з багатьох етапів (http://surl.li/amgak):

1. Оцінка масштабу та інфраструктури.
2. Прийняття рішення про спосіб впровадження.
3. Формування та затвердження технічного завдання.
4. Установка та базове налаштування SIEM-системи, тобто необхідно налаштувати SIEM-сервер, прописати логи, виконати специфічні налаштування відносно мережі підприємства.
5. Налаштування джерел подій.
6. Написання можливих додаткових правил реагування на інциденти, тому що «з коробки» SIEM-система не буде працювати належним чином.
7. Тестова експлуатація і накопичення статистики.
8. Коригування та доповнення правил кореляції.
9. Завершення тестової експлуатації.
10. Підготовка до об'єднання SIEM-систем з системами, які знаходяться на підприємстві.

На сьогоднішній день проблема впровадження виникає на перших пунктах, так як вони потребують найбільшої уваги та врахування всіх необхідних параметрів режиму їх функціонування і мають обмеження на технічне забезпечення, а також визначення великої кількості конфігураційних атрибутів, які налаштовуються в SIEM-системі. Первинне налаштування проєкту є набором дій по редагуванню конфігураційних файлів системи.

До головних задач операційного центру безпеки входять:

1. Запобігання інцидентів кібербезпеки.
2. Моніторинг, виявлення і аналіз потенційних вторгнень у режимі реального часу.
3. Реагування на підтверджені інциденти.
4. Надання відповідним організаціям актуальної інформації про поточну ситуацію, а також звітів про статус кібербезпеки, інциденти та тенденції в поведінці зловмисників.
5. Розробка і управління засобами захисту комп'ютерних мереж, такими, як IDS або системи збору / аналізу даних.

ICV 2019: 79.31
DOI 10.31494/2412-9208-2021-1-2

Додаткові можливості деяких SOC можуть включати розширений криміналістичний аналіз, криптоаналіз і зворотне проєктування шкідливих програм для аналізу інцидентів.

До ключових параметрів SOC можна віднести:

1. Організаційна модель. Дана модель створюється для малих, середніх та великих підприємств. Організаційна модель SOC буде попадати в область між командою безпеки та внутрішньо розподіленим SOC, де:

– команда безпеки визначається відсутністю окремої одиниці для виявлення або реагування на інциденти. У разі виникнення інциденту комп'ютерної безпеки збираються ресурси для вирішення проблеми, відновлення систем, після чого команда припиняє свою роботу. Цю модель, як правило, вибирають клієнти, що складаються з менше ніж 1000 користувачів або IP-адрес;

– внутрішній розподілений SOC. Постійний SOC існує, але в основному складається зі співробітників, що знаходяться за межами SOC, їх основна робота пов'язана з IT або безпекою, але не обов'язково із захистом комп'ютерних мереж. Одна людина або невелика група відповідає за координацію дій щодо забезпечення безпеки, але складні завдання виконуються особами, залученими з інших організацій. Цю модель, як правило, вибирають клієнти, що складають діапазон від 500 до 5000 користувачів або IP-адрес.

2. Виконання функцій, які виходять із завдань.

3. Рівень повноважень. SOC може володіти трьома рівнями повноважень:

– без повноважень, тобто SOC може намагатися впливати на дії, які споживачі його послуг повинні зробити. Однак у SOC немає ні формальних засобів для чинення тиску, ні вищої організаційної одиниці, здатної це зробити. Тільки замовник вирішує, розглянути або ігнорувати рекомендації SOC;

– спільні повноваження. SOC може давати рекомендації керівництву замовника, у якого є повноваження для реалізації запропонованих змін. Ці рекомендації порівнюються з пропозиціями інших зацікавлених сторін до прийняття рішення, даючи SOC можливість «висловитися»;

– усі повноваження. SOC може давати споживачам своїх послуг вказівки на певні дії, не чекаючи схвалення або підтримки з боку учасників вищого рівня.

Аналіз подій, які надходять до системи, здійснюється автоматизовано, і оператор безпеки інформується про загрозу при необхідності.

Визначені основні механізми роботи SIEM-систем за допомогою ієрархічної моделі. Під час переходу до механізмів більш високого рівня моделі кількість оброблюваних подій зменшується, а складність їх обробки збільшується див. Рис. 1.

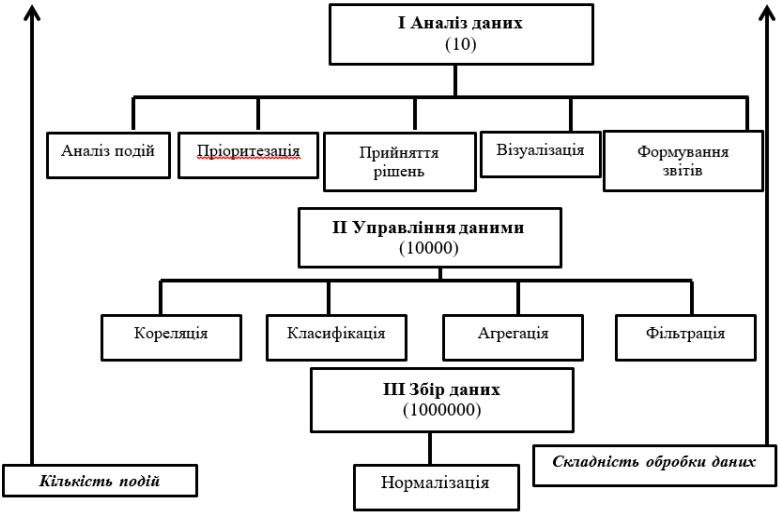

Рис. 1. Розподіл механізмів по рівням ієрархії

Перед упровадженням SIEM-проєкту в інфраструктуру SOC слід визначити, які пристрої будуть слугувати джерелами даних та виділити окремі правила кореляції:

– Кореляція на базі правил (Rule based correlation) – при впровадженні системи описується певна послідовність логічних дій, які характеризують дії зловмисника. Перевагою цього способу є висока точність виявлення зловмисника. До недоліків можна віднести необхідність періодичного оновлення правил кореляції і неможливість реагувати на послідовність подій, що не описані в правилах.

– Кореляція без використання правил (Rule lesscorrelation) – при впровадженні цього підходу всі події мають певний рейтинг, і коли рівень рейтингу послідовності подій з одним параметром (вихідний IP адреса, цільової IP адреса, користувач і т.д.) перевищує встановлений, відбувається оповіщення оператора. Перевагою цього способу є відсутність залежності від написаних правил і можливість виявлення нових векторів атак. До недоліків відноситься менший рівень точності, тому що існує ймовірність того, що незвичайні дії виконує легітимний користувач.

Наповнення SIEM-системи контентом є основним та найважливішим завданням для вирішення якого компанії необхідно мати в своєму штаті архітектора SIEM-систем, який буде налаштовувати правила в залежності від поставлених цілей, адаптувати їх під інфраструктуру та реалізовувати сценарії виявлення інцидентів.

ICV 2019: 79.31
DOI 10.31494/2412-9208-2021-1-2

Завдання 2 – чітке визначення процесів та процедур, які необхідно не тільки забезпечити тим, що будуть отримані повідомлення про кожну атаку, а ще й виконання регламенту SLA.

Розглянемо комерційний SOC.

SOC as a Service був розроблений, щоб допомогти в роботі з величезним обсягом інформації, моніторингом у режимі реального часу та реагуванням на атаки. Служба аналізує інформацію, дані й корелює події, при необхідності перетворюючи все в події, що вимагають вживання заходів. При цьому компанія ефективно використовує внутрішні IT-служби, дозволяючи їм діяти на основі конкретної інформації з урахуванням місцевих особливостей найбільш ефективним чином. У регламенті визначається чіткий поділ обов'язків між замовником і підрядником.

Малі підприємства, як правило, потребують SOC as a Service для виконання всіх функцій SOC, а великі – використовують групи аналітиків SOC as a Service як доповнення до внутрішніх команд.

Більшість великих організацій мають внутрішні SOC, у той час як компанії, що не мають персоналу або ресурсів для їх обслуговування, можуть передати деякі чи всі обов'язки SOC на аутсорсинг провайдеру керованих послуг, хмари або розміщеному віртуальному SOC (http://surl.li/amgan; Muniz, McIntyre & AlFardan, 2015; Perlroth, 2021; Yevseiev, Rzayev, Mammadova, Samedov & Romashchenko, 2018).

Під час лабораторних занять у ЦДПУ ім. В. Винниченка пропонуємо студентам проаналізувати компанії, що надають послуги операційного центру безпеки: Information Systems Security Partners (ISSP) – міжнародна компанія, що надає своїм клієнтам послуги у сфері кібербезпеки; Октава Кіберзахист – розрахована на клієнтів малого та середнього бізнесу, рівня SMB. Як технології використовує «пастки» TrapX, що дозволяють за допомогою розгорнутої архітектури забезпечити виявлення та запобігання атакам у режимі реального часу, також використовує SIEM «Splunk», безагентне рішення для захисту кінцевих точок Promisec Endpoint Manager та в якості детекторів використовує брандмауери Cisco; Infopulse – компанія, що надає аутсорсингові послуги в сфері IT в Україні; Omega Security Service – компанія пропонує комплексний захист мережевою інфраструктури, SOC нового покоління, захист від DOS/DDOS, сканує мережу на вразливість і випробування на проникнення, в тому числі з використанням методів соціальної інженерії.

Висновки. Відбулося дослідження методів, моделей та видів побудови операційних центрів безпеки під час викладання дисципліни «Безпека програм та даних». Визначені основні механізми роботи SIEM-систем за допомогою ієрархічної моделі та запроваджений механізм розподілу по рівням ієрархії.

Проаналізовані компанії, що надають послуги операційного центру безпеки, під час лабораторних занять та досліджені фактори, що впливають на підприємства при виборі типу SOC. У результаті

студентами була побудована модель SOC та класифікаційна таблиця, за допомогою якої підприємства зможуть надалі робити вибір операційного центру безпеки.

Література

Згуровський М. Проблеми інформаційної безпеки в Україні, шляхи їх вирішення // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ. – 2018. – С. 10 – 14.

Корченко А.Г. Несанкционированный доступ в компьютерные системы и методы защиты. – Киев: КМУГА, 2008.

Кузнецов О. О. Захист інформації в інформаційних системах : навч. посіб. Х. : ХНЕУ, 2018. – 510 с.

Как выявить кибератаку и предотвратить кражу денег [Електронний ресурс] – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/knowledge-base/

Guy Caspi. Why Are We Losing The Cyberwar? Forbes Technology Council Post. Jan 22, 2020. [Електронний ресурс] – Режим доступу до ресурсу: https://www.forbes.com/sites/forbestechcouncil/2020/01/22/why-are-we-losing-the-cyberwar/?sh=6cb806016b80

Jarpey, Gregory, and Scott McCoy. Security Operations Center Guidebook: A Practical Guide for a Successful SOC. Butterworth-Heinemann, 2017. – 193 p.

Managed Security Services (MSS), Worldwide Reviews and Ratings [Електронний ресурс] – Режим доступу до ресурсу: https://www.gartner.com/reviews/market/managed-security-services-worldwide

Muniz, Joseph, Gary McIntyre, and Nadhem AlFardan. Security operations center: Building, operating, and maintaining your SOC. Cisco Press, 2015.

Nicole Perlroth. How the United States Lost to Hackers. Published Feb. 6, 2021 Updated Feb. 11, 2021. [Електронний ресурс] – Режим доступу до ресурсу: https://www.nytimes.com/2021/02/06/technology/cyber-hackers-usa.html

SIEM: ответы на часто задаваемые вопросы [Електронний ресурс] – 2013. – Режим доступу до ресурсу: https://habr.com/ru/post/172389/

What Is Network Traffic Analysis [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/security/what-is-network-traffic-analysis.html

Yevseiev, S., Rzayev, K., Mammadova, T., Samedov, F., & Romashchenko, N. (2018). Класифікатор кіберзагроз інформаційних ресурсів автоматизованих банківських систем. Електронне фахове наукове видання “Кібербезпека: освіта, наука, техніка” 2(2), 47–67.

References

Zghurovskyi M. (2018). *Problemy informatsiinoi bezpeky v Ukraini, shliakhy yikh vyrishennia* [Problems of information security in Ukraine, ways to solve them]. Kyiv [in Ukrainian].

Korchenko A. (2008). *Nesanktsyonyrovannыi dostup v kompiuternыe systemы y metodы zashchyty* [Unauthorized access to computer systems and security methods]. Kyiv [in Ukrainian].

Kuznetsov O. (2018). *Zakhyst informatsii v informatsiinykh systemakh* [Protection of information in information systems: textbook]. H. : KhNEU [in Ukrainian].

Kak vыiavyt kyberataku y predotvratyt krazhu deneh [How to detect a cyberattack and prevent theft of money]. [Electronic resource]. Mode of access to the resource: https://www.ptsecurity.com/ru-ru/research/knowledge-base/

ICV 2019: 79.31
DOI 10.31494/2412-9208-2021-1-2

Guy Caspi (2020). *Why Are We Losing The Cyberwar?* [Electronic resource]. Mode of access to the resource: https://www.forbes.com/sites/forbestechcouncil/2020/01/22/why-are-we-losing-the-cyberwar/?sh=6cb806016b80

Jarpey, Gregory, and Scott McCoy (2017). *Security Operations Center Guidebook: A Practical Guide for a Successful SOC.* Butterworth-Heinemann [in United Kingdom].

Managed Security Services (MSS), Worldwide Reviews and Ratings [Electronic resource]. Mode of access to the resource: https://www.gartner.com/reviews/market/managed-security-services-worldwide

Muniz, Joseph, Gary McIntyre, and Nadhem AlFardan (2015). *Security operations center: Building, operating, and maintaining your SOC*. Cisco Press [in USA].

Nicole Perlroth (2021). *How the United States Lost to Hackers* [Electronic resource]. Mode of access to the resource: https://www.nytimes.com/2021/02/06/technology/cyber-hackers-usa.html

SIEM: otvetы na chasto zadavaemые voprosы (2013). [SIEM: answers to frequently asked questions]. [Electronic resource]. Mode of access to the resource: https://habr.com/ru/post/172389/

What Is Network Traffic Analysis [Electronic resource]. Mode of access to the resource: https://www.cisco.com/c/en/us/products/security/what-is-network-traffic-analysis.html

Yevseiev, S., Rzayev, K., Mammadova, T., Samedov, F., & Romashchenko, N. (2018). *Klasyfikator kiberzahroz informatsiinykh resursiv avtomatyzovanykh bankivskykh system* [Classifier of cyber threats of information resources of automated banking systems]. Electronic professional scientific publication “Cybersecurity: education, science, technology” Kyiv [in Ukrainian].

АНОТАЦІЯ

У дослідженні розглядається операційний центр безпеки (Security Operations Center), який забезпечує виявлення та аналіз кібербезпеки, оперативне реагування, запобігання виникненню кібератак. Для забезпечення видимості та надання аналітикам можливості захисту від атак використовуються технології Security Operations Center.

Показаний алгоритм подання теми «Центр забезпечення безпеки» під час викладання дисципліни «Безпека програм та даних» у Центральноукраїнському державному педагогічному університеті імені Володимира Винниченка, а саме розглядаються проблеми впровадження систем моніторингу подій Security information and event management, види операційних центрів, методи побудови внутрішніх операційних центрів безпеки.

Формуються в студентів предметні компетентності: класифікувати, ідентифікувати і захищати засоби обробки інформації від несанкціонованого доступу та комп’ютерних вірусів, розробляти індивідуальні системи управління доступом і захистом інформації.

Показаний процес впровадження Security information and event management-систем на підприємство, основні механізми роботи цієї системи за допомогою ієрархічної моделі, головні задачі операційного центру безпеки, ключові параметри Security Operations Center (організаційна модель; виконання функцій, які виходять із завдань; рівень повноважень), основні правила кореляції.

Розглянутий комерційний операційний центр безпеки SOC as a Service, який розроблений, щоб допомогти в роботі з величезним обсягом інформації, моніторингом в режимі реального часу та реагуванням на атаки.

Студентами, під час лабораторних занять, проаналізовані компанії, що надають послуги операційного центру безпеки (Information Systems Security Partners, Октава Кіберзахист, Infopulse, Omega Security Service) та досліджені фактори, що впливають на підприємства при виборі типу Security Operations Center.

Ключові слова: *операційний центр безпеки, SEIM-системи, кібербезпека, SOC as a Service.*

ICV 2019: 79.31
DOI 10.31494/2412-9208-2021-1-2