CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

DOI 10.20535/2411-1031.2019.7.2.190570
УДК 004.056.53

ІГОР СУБАЧ,
АРТЕМ МИКИТЮК,
ВОЛОДИМИР КУБРАК

АРХІТЕКТУРА ТА ФУНКЦІОНАЛЬНА МОДЕЛЬ ПЕРСПЕКТИВНОЇ ПРОАКТИВНОЇ ІНТЕЛЕКТУАЛЬНОЇ SIEM-СИСТЕМИ ДЛЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У статті розглядаються актуальні, у теперішній час, питання кіберзахисту об'єктів критичної інфраструктури, які набувають все більшої важливості. На підставі проведеного аналізу зроблено висновок про те, що основою побудови ефективної системи кіберзахисту є застосування систем управління інформацією та подіями безпеки (SIEM-систем). Застосування систем даного типу дозволяє не тільки виявляти кіберінциденти, а й прогнозувати їх на основі накопичених в системі даних. Запропонована нова архітектура перспективної проактивної інтелектуальної SIEM-системи, яка, додатково до традиційних рівнів – збору, управління та аналізу даних, включає четвертий рівень - рівень прийняття та реалізації рішень. Реалізація запропонованої архітектури є можливою на шляхом розробки та застосування нових методів нормалізації, фільтрації, класифікації, агрегації, кореляції, пріоритезації та аналізу подій і кіберінцидентів, їхніх наслідків, генерації різноманітних звітів, повідомлень та візуального представлення даних для оперативного та обґрунтованого прийняття рішень і реалізації їх на основі технологій інтелектуального аналізу даних, машинного навчання, обробки великих даних (Big Data) та штучного інтелекту. Запропонована нова функціональна модель перспективної інтелектуальної SIEM-системи, яка включає: підсистему збору та первинної обробки даних з різнорідних джерел; підсистему управління даними; підсистему аналізу даних і підсистему прийняття та реалізації рішень. Реалізація на практиці моделі дозволяє мінімізувати участь людини під час вирішення задачі реагування на кіберінциденти, тим самим підвищуючи оперативність та обґрунтованість рішень, які вона приймає Застосування запропонованих нової архітектури проактивної інтелектуальної SIEM-системи та її функціональної моделі, дозволяє зробити новий крок в еволюції систем даного типу у бік підвищення ефективності їх використання в системах кіберзахисту об'єктів критичної інфраструктури.

Ключові слова: критична інфраструктура, кіберзахист, SIEM-система, прийняття рішень

Постановка проблеми. В умовах стрімкої диджиталізації різних сфер людської діяльності, питання кіберзахисту об'єктів критичної інфраструктури набувають особливої важливості, адже порушення штатних режимів їхнього функціонування та виведення їх з ладу можуть привести до непоправних наслідків. Відповідно до [1] під критичною інфраструктурою розуміють сукупність критично важливих об'єктів діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки та оборони України, навколишнього середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей.

Відповідно до переліку вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури [2], значна увага приділяється питанням реєстрації подій їхніми компонентами, а саме: компоненти об'єкту повинні здійснювати реєстрацію та збереження в електронних журналах інформацію про події, що пов'язані із роботою користувачів, зміну конфігураційних налаштувань, спроб несанкціонованого доступу до ресурсів об'єкту; журнали реєстрації подій повинні містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події; на об'єкті повинна бути система збору та аналізу журналів реєстрації подій, що включає функції фільтрування накопиченої в них інформації для здійснення її вибірки й аналізу за різними критеріями та мати інтерфейс з іншими системами.

Аналіз останніх досліджень і публікацій показує, що основою побудови ефективної системи кіберзахисту об'єктів критичної інфраструктури має бути застосування SIEM-систем (Security Information and Event Management) – систем управління інформацією та подіями безпеки. Застосування в контурі захисту SIEM-системи дозволяє ефективно задовольняти вимогам, що наведені вище та здійснювати проактивне управління кіберінцидентами, тобто шляхом застосування автоматизованих механізмів, які використовують інформацію про події, що вже відбулися в системі, прогнозувати майбутні події, які будуть відбуватися в ній, а також адаптувати параметри захисту системи до її поточного стану, тим самим здійснюючи превентивні заходи ще до того, коли ситуація в системі стане критичною [3]. Відповідно до цього SIEM-система повинна вирішувати комплекс задач, до яких можна віднести наступні [4]:

- збір, обробку та аналіз подій безпеки, що поступають до неї з множини різнорідних розподілених джерел;
- виявлення в режимі реального часу або близького до нього кібератак та порушень політики безпеки;
- проведення розслідування кіберінцидентів;
- формування ефективних рішень щодо кіберзахисту системи;
- формування звітних документів і візуалізацію стану системи та інші.

Для вирішення даних задач, SIEM-система, на підставі зібраних з журналів (log-файлів) початкових даних, які накопичують інформацію про події, що відбуваються в системі, відбирає такі, що можуть бути ознаками кібератак або інших небажаних дій в системі.

У відповідності до поставлених перед SIEM-системою задач та функцій, які вона повинна виконувати, її архітектура має бути багаторівневою та включати наступні рівні [5]: рівень збору даних, рівень управління даними та рівень аналізу даних.

На першому рівні агенти SIEM-системи з різнорідних джерел (IPS-систем, міжмережевих екранів, антивірусного програмного забезпечення, журналів операційних систем та систем керування базами даних, сенсорів системи) збирають первинні дані про події в системі, здійснюють їхню первинну обробку та фільтрацію [6, 7].

Далі, на другому рівні, здійснюється управління даними про події безпеки, які були зібрані та відфільтровані раніше, накопичені у сховищі даних (репозитарії) системи та представляються в якості початкових даних для механізмів їхнього аналізу, які реалізовано в системі.

На третьому рівні, сервер додатків, на підставі даних, що накопичуються в сховищі даних системи, аналізує їх та перетворює до вигляду, який є придатним для здійснення повідомлень про кібератаки та інші негативні події, що відбуваються в системі, а також відпрацювання рішень щодо кіберзахисту системи: звітів у заздалегідь визначеній та довільній формі та різних моделей візулазіції даних про події, які відбуваються в системі.

Проте аналіз сучасного стану розвитку SIEM-систем показує [8], що управління безпекою не повинно обмежуватися тільки стадією виявлення загроз. Вони повинні застосовувати новітні інформаційні технології підтримки прийняття рішень [9, 10], які ґрунтуються на методах штучного інтелекту, машинного навчання та інтелектуального

аналізу даних для реагування на кіберінциденти на основі звітів про стан системи безпеки та оцінки можливих ризиків, а також автоматизованого реагування на них. Згідно досліджень компанії Gartner [8], лідерами на ринку SIEM-систем є рішення від компаній: Splunk, IBM, LogRhythm, Dell Technologies (RSA), Exabeam, McAfee та Securonix. До критеріїв оцінювання сучасних SIEM-систем [8] додаються такі, як моніторинг безпеки в режимі реального часу, аналітика стану захищеності системи, управління кіберінцидентами та реагування на них.

Виходячи з цього, архітектура перспективної SIEM-системи повинна, на додаток до наведених, включати четвертий рівень – рівень прийняття та реалізації рішень.

Метою роботи є розробка архітектури та функціональної моделі перспективної проактивної інтелектуальної системи управління інформацією та подіями безпеки для кіберзахисту об'єктів критичної інфраструктури.

Виклад основного матеріалу дослідження. Реалізація наведеної архітектури SIEM-системи, може бути здійсненою шляхом розробки та практичної реалізації різних методів, які відповідають її певним рівням та таких як: нормалізація, фільтрація, класифікація, агрегація, кореляція, пріоритезація та аналіз подій і кіберінцидентів, їхніх наслідків, генерація різноманітних звітів, повідомлень та візуального представлення даних для оперативного та обґрунтованого прийняття рішень.

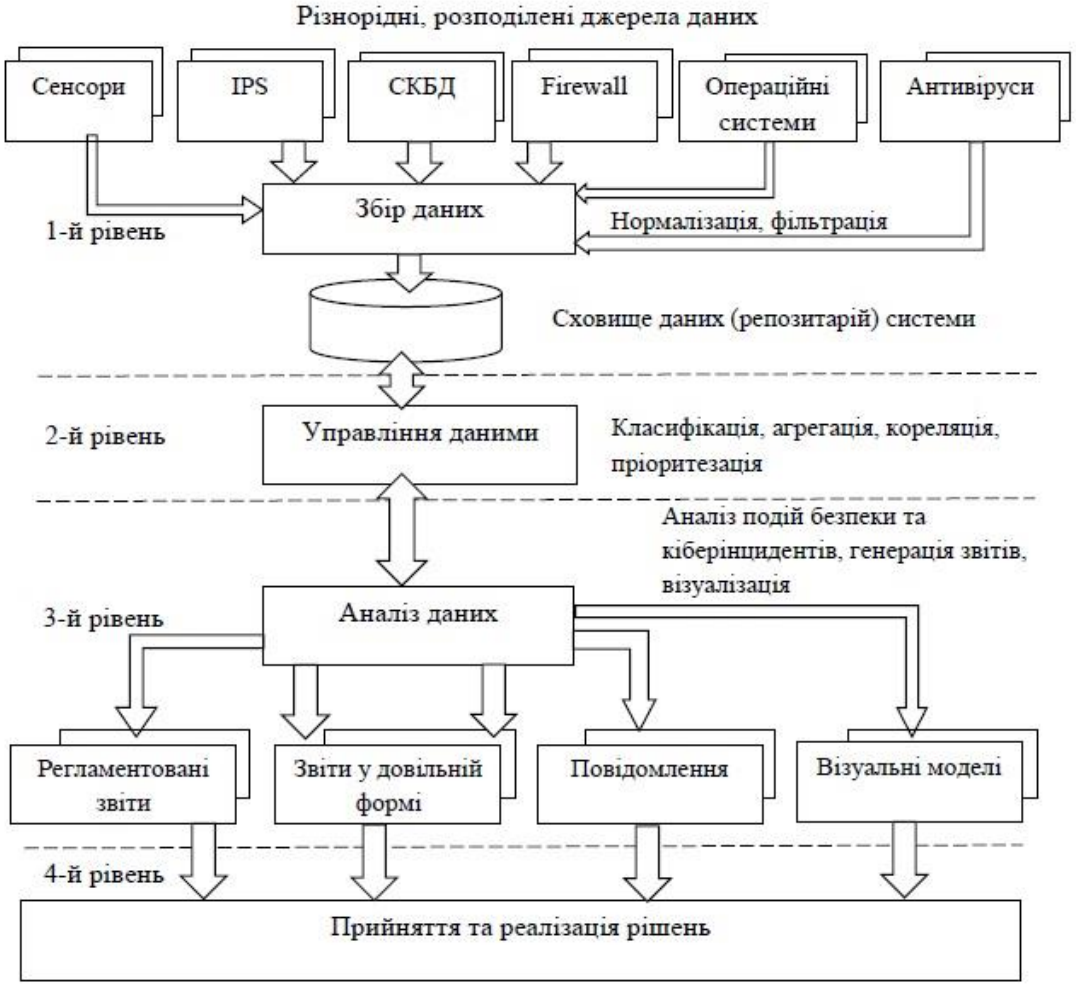

Рисунок 1 – Архітектура перспективної проактивної SIEM-системи

Суть застосування даних методів полягає у наступному [4]. Під час нормалізації здійснюється приведення записів журналів, що зібрані з різнорідних джерел до єдиного формату, для подальшого накопичення у сховищі даних системи для подальшої обробки.

Фільтрація подій безпеки передбачає видалення з системи подій, що не є перспективними для подальшого аналізу та обробки.

Класифікація дозволяє на основі атрибутів подій безпеки віднести їх до заздалегідь визначених класів.

Під час агрегації здійснюється об'єднання подій безпеки за їхніми ознаками.

Методи кореляції дають змогу знаходити взаємозв'язки між різними подіями в системі, що, у свою чергу, дозволяє виявляти кібератаки, а також нештатні події, що пов'язані з порушенням політики безпеки.

Методи пріоритезації (шляхом застосування створених в системі правил) дозволяють визначити рівень значимості та критичності подій безпеки.

Аналіз подій безпеки, кіберінцидентів та їхніх наслідків, передбачає моделювання кібератак та їх наслідків, аналіз уразливостей системи, визначення параметрів порушників, оцінку ризиків, прогнозування подій безпеки та кіберінцидентів.

Під час генерації регламентованих і довільних звітів та повідомлень здійснюється інформування про параметри функціонування системи.

Методи візуалізації застосовуються для представлення в графічному виді даних, які характеризують результати аналізу подій безпеки в системі та її основних елементів.

Та, відповідно, прийняття та відпрацювання рішень полягає у здійсненні певних дій щодо реконфігурування засобів захисту системи щодо припинення або запобігання кібератакам та відновлення штатного режиму функціонування системи.

Таким чином, функціональна модель перспективної проактивної SIEM-системи може бути представлена у наступному виді:

$$M_{SIEM} = \langle COL, CON, ANL, DEC \rangle, \quad (1)$$

де $COL = \left\langle \{PUR\}_{i=1}^{n}, NOR \right\rangle$ – підсистема збору та первинної обробки даних з різнорідних джерел: $\{PUR\}_i, i = \overline{1,n,}$ – множина модулів завантаження даних з різнорідних джерел; NOR – модуль нормалізації даних (приведення різних форматів даних до єдиного формату для внутрішнього зберігання);

$CON = \langle FIL, CLS, AGR, COR \rangle$ – підсистема управління даними: FIL – модуль фільтрації подій (видалення неважливих для аналізу подій); CLS – модуль класифікації подій на заздалегідь визначені класи; AGR – модуль агрегації подій до більш узагальненого рівня;

COR – модуль кореляції подій (знаходження взаємозв'язків між різними подіями);

$ANL = \left\langle MDL, PRI, \{GEN\}_{j=1}^{m}, \{VIZ\}_{k=1}^{l} \right\rangle$ – підсистема аналізу даних: MDL – модуль моделювання кібератак і кіберінцидентів та їх прогнозування; PRI – модуль пріоритезації (визначення важливості подій безпеки); $\{GEN\}_j, j = \overline{1,m,}$ – множина модулів генерації регламентованих та нерегламентованих звітів; $\{VIZ\}_{k=1}^{l}$ – множина модулів візуалізації даних;

DEC – підсистема прийняття та реалізації рішень.

Взаємозв'язок підсистем та методів, що забезпечують їх функціонування наведено на рис.2.

Основними функціями, які виконує підсистема прийняття та реалізації рішень є:

- допомого офіцеру безпеки в оцінці ситуації, яка склалася в системі;
- генерація можливих рішень (сценаріїв дій) для обслуговуючого персоналу системи щодо реагування на кіберінциденти;
- оцінка та допомога офіцеру безпеки у виборі найкращого сценарію реагування на кіберінцидент;
- здійснення постійного обміну інформацією під час підготовки та прийняття рішень, а також узгодженні групових рішень обслуговуючого персоналу;

– моделювання рішень, що приймаються офіцерами безпеки;
– динамічне прогнозування та аналіз можливих наслідків (ризиків) від рішень, що приймаються щодо реагування на кіберінциденти;
– збір даних про результати реагування на кіберінциденти та їхню оцінку;
– донавчання системи на основі аналізу результатів рішень, які були прийняті щодо реагування на кіберінциденти та їхньої оцінки.

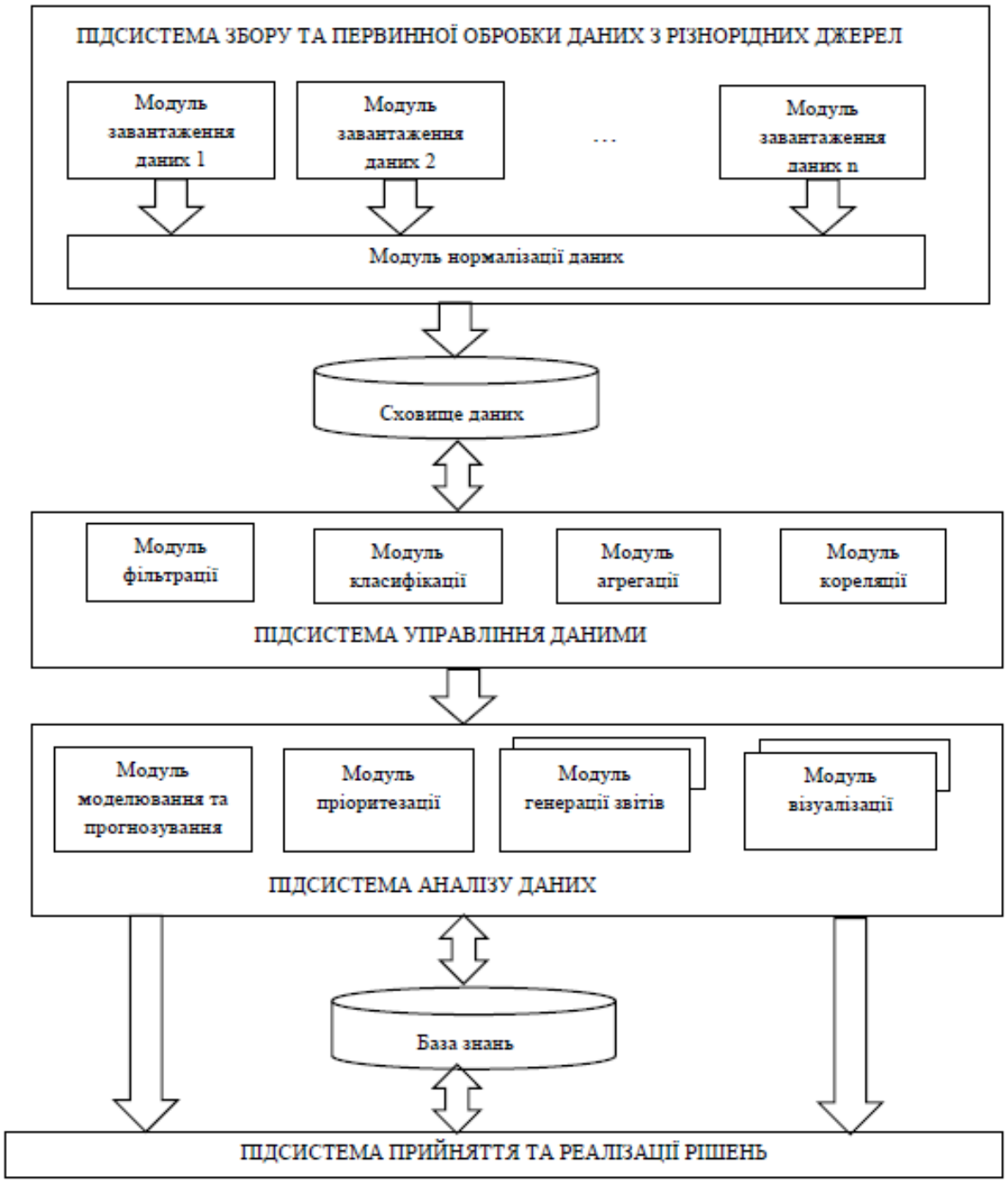

Рисунок 2 – Функціональна модель перспективної проактивної інтелектуальної SIEM-системи

Слід зауважити, що саме введення до моделі підсистеми прийняття та реалізації рішень, дозволяє мінімізувати участь людини під час вирішення задачі реагування на кіберінциденти, тим самим підвищуючи оперативність та обґрунтованість рішень, які вона приймає [9].

Це, у свою чергу, приводить до підвищення ефективності системи кіберзахисту, знижує ризики під час застосування SIEM-систем на основі аналізу великих даних, оперативного реагування на кіберінциденти та підвищення продуктивності роботи SIEM-системи.

Висновки. Застосування запропонованої в роботі нової архітектури проактивної інтелектуальної системи управління інформацією та подіями безпеки, що включає рівень прийняття та реалізації рішень, дозволяє зробити новий крок у подальшій еволюції систем даного типу у бік підвищення ефективності їх використання у системах кіберзахисту об'єктів критичної інфраструктури.

Розроблена та запропонована в роботі нова функціональна модель даної системи, що включає підсистему збору та первинної обробки даних з різнорідних джерел, підсистему управління даними, підсистему аналізу даних та підсистему прийняття та реалізації рішень є основою для подальших наукових досліджень щодо створення ефективної системи кіберзахисту об'єктів критичної інфраструктури.

Перспективними напрямками подальших наукових досліджень є розробка функціональної структури підсистеми прийняття та реалізації рішень проактивної інтелектуальної SIEM-системи та методів, що забезпечують її функціонування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Верховна рада України. 7 Сесія. (2017, Жовт. 5). *Закон України № 2163-VIII, Про основні засади забезпечення кібербезпеки України.* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/2163-19. Дата звернення: Верес. 10, 2019.

[2] Кабінет міністрів України. (2019, Черв. 19). *Постанова Кабінету Міністрів України № 518, Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури.* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF. Дата звернення: Верес. 10, 2019.

[3] И.В. Котенко, В.В. Воронцов, А.А. Чечулин, и А.В. Уланов, "Проактивные механизмы защиты от сетевых червей: подход, реализация и результаты экспериментов", *Информационные технологии*. №1, с. 37 – 42, 2009.

[4] И.В. Котенко, И.Б. Саенко, О.В. Полубелова, и А.А. Чечулин, "Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах", *Труды СПИИРАН*, Вып. 1(20), с. 27 – 56, 2012.

[5] M. Stevens, "Security Information and Event Management (SIEM). Presentation, in Proc. The NEbraska, CERT Conference. [Online]. Available: http://www.certconf.org/presentations/ 2005/files/WC4.pdf. Accessed on: Sept. 09, 2019.

[6] І.Ю. Субач, В.В. Фесьоха, та Н.О. Фесьоха, "Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі, відкритих на основі загальнодоступних ліцензій", *Information Technology and Security*, vol. 5, iss. 1, pp. 29–41, 2017.

[7] R. Shanmugavadivu, and N. Nagarajan, "Network intrusion detection system using fuzzy logic", *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 2, №1, pp. 101–111, 2011.

[8] K. Kavanagh, T. Bussa, and G. Sadowski, "Magic Quadrant for Security Information and Event Management". [Online]. Available: https://virtualizationandstorage.files.wordpress.com/ 2018/03/magic-quadrant-for-security-information-and-event-3-dec-2018.pdf. Accessed on: Sept. 17, 2019.

[9] Б.М. Герасимов, та І.Ю. Субач, "Показники якості інформаційного забезпечення та їх вплив на ефективність застосування систем підтримки прийняття рішень", *Вісник КНУ ім. Т. Г. Шевченка*, Вип. № 20, с. 27–29, 2008.

[10] Б.М. Герасимов, І.Ю. Субач, та Є.В. Нікіфоров, "Моделі надання знань для використання в системах підтримки прийняття рішень", *Науково-технічна інформація*. №1, с.7–11, 2005.

Стаття надійшла до редакції 24.09.2019.

REFERENCE

[1] Verkhovna Rada Information. 7th session. (2017, Okt. 5), *Law of Ukraine № 2163-VIII, On the Fundamental Principles of Cyber Security of Ukraine*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2163-19. Accessed on: Sept. 10, 2019.

[2] Cabinet of Ministers of Ukraine. (2019, June 19). *Resolution of the Cabinet of Ministers of Ukraine № 518, General requirements for cyber defense of critical infrastructure: official publication.* [Online]. Available: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF. Accessed on: Sept. 10, 2019.

[3] I.V. Kotenko, V.V. Voroncov, A.A. Chechulin, and A.V. Ulanov, "Proactive security mechanisms against network worms: approach, implementation and results of the experiments", *Information Technology*, no. 1, pp. 37–42.

[4] I. Kotenko, I. Saenko, O. Polubelova, and A. Chechulin, "Application of security information and event management technology for information security in critical infrastructures", *SPIIRAS Proceeding*, iss. 1 (20), pp. 27–56.

[5] M. Stevens, "Security Information and Event Management (SIEM). Presentation, in Proc. The NEbraska, CERT Conference. [Online]. Available: http://www.certconf.org/presentations/ 2005/files/WC4.pdf. Accessed on: Sept. 09, 2019.

[6] I. Subach, V. Fesokha, and N. Fesokha, "An analysis of existing decisions to prevent intrusion in information and telecommunication networks open on the basis of public licenses", *Information Technology and Security*, vol. 5, iss. 1, pp. 29–41, 2017.

[7] R. Shanmugavadivu, and N. Nagarajan, "Network intrusion detection system using fuzzy logic", *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 2, №1, pp. 101 – 111, 2011.

[8] K. Kavanagh, T. Bussa, and G. Sadowski, "Magic Quadrant for Security Information and Event Management". [Online]. Available: https://virtualizationandstorage.files.wordpress.com/ 2018/03/magic-quadrant-for-security-information-and-event-3-dec-2018.pdf. Accessed on: Sept. 17, 2019.

[9] I. Subach, and B. Gerasimov, "Quality indicators of information support and their impact on the effectiveness of decision support systems", *Bulletin of Taras Shevchenko National University of Kiev*, no. 20, pp. 27–29, 2008.

[10] I. Subach, B. Gerasimov, E. Nikiforov, "Models of knowledge delivery for use in decision support systems", *Scientific and technical information*, №1, pp. 7–11, 2005.

IHOR SUBACH,
ARTEM MYKYTIUK,
VOLODYMYR KUBRAK

ARCHITECTURE AND FUNCTIONAL MODEL OF A PERSPECTIVE PROACTIVE INTELLECTUAL SIEM FOR CYBER PROTECTION OF OBJECTS OF CRITICAL INFRASTRUCTURE

The article deals with the current, nowadays, issues of cyber defense of critical infrastructure, which are becoming increasingly important. Based on the analysis, it is concluded that the basis of building an effective cyber defense system is the use of information management and security event management (SIEM). The use of systems of this type allows not only to detect cyber security incidents, but also to predict them based on the accumulated data in the system. The proposed new architecture for a promising proactive smart SIEM, which, in addition to the traditional levels of data collection, management and analysis, includes the fourth level - the level of decision making and implementation. The implementation of the proposed architecture is possible through the development and application of new methods of normalization, filtering, classification, aggregation,

correlation, prioritization and analysis of events and cyber security incidents, their consequences, generation of various reports, messages and visual presentation of data for operational and substantiated adoption based on data mining technologies, machine learning, Big Data processing and artificial intelligence. A new functional model of a promising intelligent SIEM is proposed, which includes: subsystem of collection and primary processing of data from heterogeneous sources; data management subsystem; the data analysis subsystem and the decision and implementation subsystem. The implementation of the model allows to minimize human participation in solving the problem of responding to cyber incidents, thereby increasing the efficiency and validity of the decisions it makes. The application of the proposed new architecture of a proactive intellectual SIEM and its functional model, allows to take a new step in the evolution of type towards increasing the efficiency of their use in cyber defense systems of critical infrastructure.

Key words: cyber protection, critical infrastructure, SIEM, making decisions.

Ігор Юрійович Субач, доктор технічних наук, доцент, завідувач кафедри, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0002-9344-713X.

E-mail: igor_subach@ukr.net

Микитюк Артем В'ячеславович, аспірант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0002-8307-9978.

E-mail: mukuta8888@gmail.com

Кубрак Володимир Олександрович, аспірант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0001-8877-5289.

E-mail: volodymir.kubrak@ukr.net

Subach Ihor, doctor of technical science, associate professor, head of department, Institute of special communications and information security National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Mykytiuk Artem, postgraduate student, Institute of special communications and information security National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Kubrak Volodymyr, postgraduate student, Institute of special communications and information security National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.