УДК 004.056.53:004.2-047.36 DOI: 10.31673/2412-4338.2024.040224

Корнієць Віктор Анатолійович
Інститут проблем математичних машин і систем Національної академії наук України, Київ
ORCID 0000-0002-4967-8395

Складанний Павло Миколайович
Київський столичний університет імені Бориса Грінченко, Київ
ORCID 0000-0002-7775-6039

ФОРМУВАННЯ ВИМОГ ДО АРХІТЕКТУРИ І ФУНКЦІЙ СИСТЕМ МОНІТОРИНГУ КІБЕРБЕЗПЕКИ

Анотація. *У статті розглянуто проблеми і задачі формування вимог до архітектури і функцій систем моніторингу кібербезпеки. Системи моніторингу кібербезпеки в сучасних інформаційно-комунікаційних системах, з одного боку, виконують важливе завдання забезпечення збору і аналізу даних щодо реалізації кібератак та оперативного їх виявлення. З іншого боку, вони виступають в якості інструменту дослідження вразливостей та умов реалізації атак у ході проведення розслідувань кіберінцидентів, які відбулись, с метою визначення адекватних організаційно-технічних контрзаходів та їх оперативного впровадження. В роботі на основі теорії статистичних рішень пропонуються дві важливих характеристики систем моніторингу кібербезпеки, а саме: селективність та чутливість. Селективність системи моніторингу визначається ймовірністю помилки першого роду у випадку розрізнення двох гіпотез: H_0 що відповідає звичайному стану функціонування автоматизованої системи та гіпотези H_1, яка відповідає ситуації що виникає у випадку реалізації кібератаки. Чутливість в роботі визначається ймовірністю помилки другого роду, коли вважається вірною гіпотеза H_0, хоча насправді вірна її альтернатива. Ще одним важливим кількісним показником системи моніторингу визнана затримка часу реагування на події в автоматизованій системі, від якої цілком залежить оперативність прийняття менеджментом кібербезпеки. Зважаючи на вплив рішень, які приймаються системою моніторингу на загальний стан кібербезпеки організації визначено, що ця система має бути захищена в плані забезпечення конфіденційності та цілісності інформації накопичується, обробляється та зберігається в системі. В роботі запропоновані також інші характеристики систем моніторингу, які є важливими з точки їх оцінювання та сертифікації.*

Ключові слова. *система моніторингу кібербезпеки, кібербезпека, загроза, захист інформації, конфіденційність, цілісність, SIEM, LMS.*

Viktor Korniiets
Institute of Problems of Mathematical Machines and Systems, *Kyiv*
ORCID 0000-0002-4967-8395

Pavlo Skladannyi
Borys Grinchenko Kyiv Metropolitan University, Kyiv
ORCID 0000-0002-7775-6039

FORMATION OF REQUIREMENTS FOR THE ARCHITECTURE AND FUNCTIONS OF CYBER SECURITY MONITORING SYSTEMS

Abstract. *The article addresses the challenges and tasks of formulating requirements for the architecture and functions of cybersecurity monitoring systems. These systems, in modern information and communication systems, serve two essential purposes. On one hand, they play a critical role in collecting and analyzing data related to cyberattacks and their timely detection. On the other hand, they act as a tool for studying vulnerabilities and attack conditions during cyber incident investigations to determine adequate organizational and technical countermeasures and ensure their prompt implementation. Based on statistical decision theory, the paper proposes two critical characteristics of cybersecurity monitoring systems:*

selectivity and sensitivity. The selectivity of a monitoring system is defined by the probability of a Type I error when distinguishing between two hypotheses: H_0, corresponding to the normal functioning state of an automated system, and H_1, representing a scenario where a cyberattack is being executed. Sensitivity is defined by the probability of a Type II error, where H_0 is considered correct, despite the actual validity of its alternative. Another significant quantitative metric identified is the response time delay to events within an automated system, which directly impacts the operational efficiency of cybersecurity management. Given the influence of decisions made by the monitoring system on an organization's overall cybersecurity state, the system must ensure the confidentiality and integrity of the information accumulated, processed, and stored. The paper also proposes additional characteristics of monitoring systems that are crucial for their evaluation and certification.

Keywords: *cybersecurity monitoring system, cybersecurity, threat, information protection, confidentiality, integrity, SIEM, LMS.*

1. Вступ

Досвід останніх років свідчить, що впровадження в сучасних системах кібербезпеки програмно-апаратних комплексів моніторингу їх стану та відстеження розвитку подій в кіберпросторі суттєво підвищує ефективність діяльності менеджменту безпеки що спрямована на покращення кіберзахисту критичної інфраструктури, створення корпоративних центрів безпеки, проведення аналізу подій, що відбулись з метою вироблення рекомендацій з реалізації контрзаходів.

На поточний час існує багато продуктів різних виробників, що підтримують різноманітні потреби потенційних користувачів, зручність використання, здатність інтегруватися з іншими рішеннями захисту, цінова політика та особливості. [1].

Водночас можливо констатувати, що комплексної методики оцінки характеристик систем моніторингу безпеки та опису відповідних продуктів як набору вимірів, що визначають їх ключові властивості – здатність з мінімальною помилкою виявляти реальні кіберінциденти не існує.

Системи моніторингу переважно не розглядаються як специфічний об’єкт атак в комп’ютерних системах, що потенційно робить їх вразливими до атак модифікації та підміни даних, виявлення кордонів захисту, дослідження методології реагування на інциденти та вилучення іншої конфіденційної інформації з накопичуваних масивів даних.

З урахуванням викладеного уявляється доцільним проаналізувати цю ситуацію та визначити напрями покращення ефективності використання ресурсів систем моніторингу та підвищення їх власної безпеки.

2. Постановка проблеми

Незважаючи на те, що у сфері впровадження та використання систем моніторингу кібербезпеки інформаційно-комунікаційних технологій на даний час досягнуто значного прогресу, проблема формування вимог до систем нового покоління залишається дуже актуальною.

3. Аналіз останніх досліджень і публікацій

Одним з джерел інформації для роботи систем моніторингу безпеки є лог-файли або файли журналів подій, які спочатку використовувались як інструмент налаштування компютерної системи, оскільки вони містять інформацію про події на серверах і робочих станціях, їх взаємодії, дані про дії користувачів, про помилки програм і обладнання тощо.

Поширення мережевих технологій, повсюдний доступ до глобальної мережі Інтернет актуалізували задачу аналізу даних в лог-файлів [2].

Великий обсяг відповідних даних, складність їх ручної обробки актуалізували проблему стандартизації процедур та підходів до цього. Відповіддю на це стало патентування [3] відповідного рішення, що отримало назву системи управління журналами (Log Management System – LMS).

Важливим етапом розвитку продуктів з моніторингу безпеки стало поширення систем управління безпекою та подіями безпеки (Security Information and Event Management – SIEM),

застосування яких в корпоративних центрах безпеки та хмарних середовищах стало практично повсюдним рішенням. Зокрема, в [4] системно оцінені основні принципи та технічні вимоги до реалізації та розгортання продуктів SIEM в хмарному середовищі.

Виходячи з практики та досвіду забезпечення інформаційної безпеки в [5] для SIEM запропонована комплексна методологія оцінювання, що базувалась на критеріях, які переважно визначені в аспекті функціональності систем.

Поглиблений аналіз трендів розвитку та застосування SIEM на об'єктах критичної інфраструктури (Critical Infrastructures) наданий в [6]. При цьому в роботі досліджені поширені SIEM у розумінні їх критичної функціональності та надано аналіз зовнішніх факторів, що впливають на ландшафт систем моніторингу в перспективі. В рамках огляду існуючих рішень також надано перелік потенційних удосконалень для наступного покоління SIEM, а також здійснено аналіз переваг їх використання на об'єктах критичної інфраструктури.

У [7], [8] розглядаються питання еволюції SIEM на основі застосування технології штучного інтелекту з метою підвищення якості виявлення інцидентів та їх аналізу на основі лог-файлів, а також реагування.

У [9] досліджена проблема масштабування LMS архітектури на основі блокчейн мережі, але запропоноване рішення не враховує той фактор, що ідея блокчейн базується на надлишковості такої мережі, що потребує відповідних матеріальних та енергетичних витрат.

У [10] запропонована, на думку авторів, ефективна архітектура побудова системи SIEM, але особливості реалізації механізмів обробки первинних даних, включаючи їх фільтрацію, нормалізацію , агрегацію і кореляцію залишились поза межами дослідження, що суттєво ускладнює розуміння запропонованих переваг.

У роботі [11] запропонована інтеграція SIEM з прогнозною аналітикою, що може давати певний ефект у плані вирішення поставлених перед системою завдань, але відсутність докладної інформації щодо застосованих математичних рішень на ключових етапах обробки даних ускладнює можливість застосування запропонованого методу для реалізації процедур оцінювання відповідності.

Метою статті є формування переліку вимог та напрацювання технологічних рішень що доцільно впровадити в системи моніторингу нового покоління та використовувати під час реалізації процедур оцінювання відповідності таких систем сучасним вимогам.

4. Методологічні засади дослідження

Забезпечення ефективного функціонування гарантоздатних автоматизованих систем об'єктів критичної інфраструктури потребує реалізації двох процедур що є складовими їхніх систем кіберзахисту, а саме:

– надійного оперативного виявлення ознак виникнення інцидентів, які можуть підвищувати ризики порушення певних технологічних процесів;

– системного дослідження причин та умов реалізації кіберзагроз з метою впровадження додаткових контрзаходів або вдосконалення вже існуючих рішень.

Для автоматизації процесу збирання, обробки та аналізу інформації про кіберінциденти на поточний час використовуються комплекси програмно-апаратних засобів – системи моніторингу подій [1] як платформи для управління безпекою інформаційно-комунікаційних систем (ІКС).

Залежно від архітектури та функціональних можливостей розрізняють два основних програмно-апаратних рішення подібного типу, саме:

– система управління лог-файлами LMS (Log Management System), яка збирає, обробляє візуалізує дані з журналів подій – логів (операційних систем, прикладних програм тощо) з декількох хостів та систем забезпечуючи менеджемент безпеки вихідними даними для опрацювання визначених вище задач;

– система інформаційної безпеки та управління подіями SIEM (Security information and Event Management), яка на підставі аналогічної інформації (включаючи дані від засобів кіберзахисту)яка забезпечує в автоматизованому режимі можливість прийняття рішень щодо

подій безпеки. За її допомогою хости здатні генерувати звіти про вразливості в системі захисту.

Джерелами інформації для прийняття організаційно-технічних рішень в рамках визначених процедур є пристрої та обладнання комп'ютерних систем, різноманітні журнали обліку дій та подій, в яких можуть реєструватись різні дані щодо їх часових рамок, ідентифікатори суб'єктів - ініціаторів, їх мережні адреси тощо.

Великий обсяг вхідної інформації в системах моніторингу та аналізу подій в розподілених інформаційно-комунікаційних системах (рис. 1) потребує попередньої її обробки за допомогою процедур фільтрації з метою видалення шуму, що обумовлений випадковими процесами та подіями, що не пов'язані з кіберінцидентами.

Отримані дані для покращення умов їх подальшої обробки зазнають нормалізації, яка спрямована забезпечення їх єдиного формату та структури. Процедури нормалізації забезпечують уніфікацію подання даних, які отримуються від різних джерел, що покращують їх подальшу інтерпретацію, усувають можливу неоднозначність та зменшує надлишковість за рахунок усунення зайвих полів, дублювання та помилок. Особливо слід зауважити, що нормалізація підвищує ефективність процедур кореляції подій, інформація про які отримана з різних джерел.

Підвищенню ефективності кореляції подій сприяють процедури агрегації (об'єднання) даних, які на підставі визначених критеріїв (наприклад, тип подій, час виникнення, джерело походження тощо) надають можливість підвищити інформативність даних від розрізнених джерел, що сприяє скороченню часу на виявлення аномалій та тенденцій, виявленню складних кібератак та інцидентів.

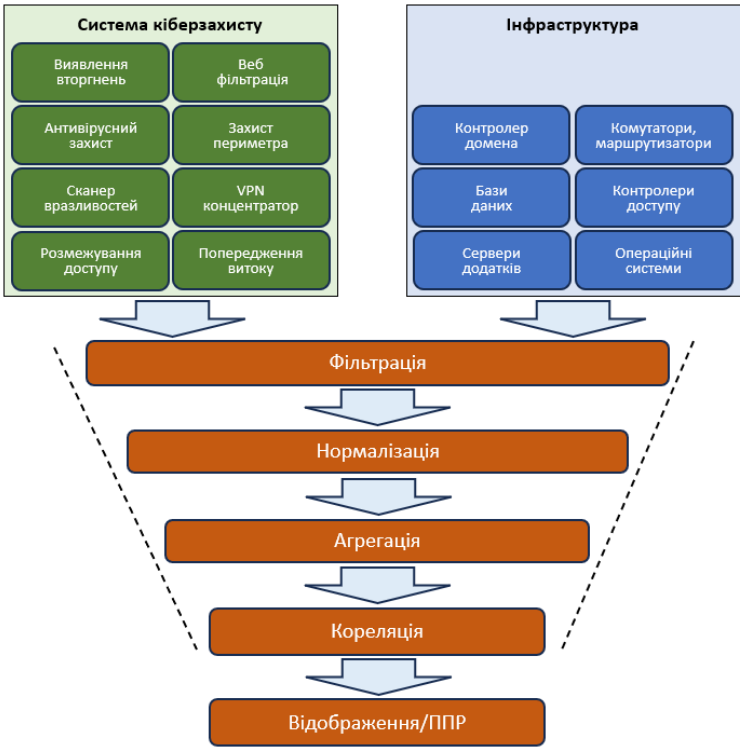

Рис. 1 Архітектура системи моніторингу подій в ІКС

Кореляція подій в SIEM дозволяє встановлювати взаємозв'язок між подіями, дані щодо яких отримані з різних складових інформаційної інфраструктури та системи кіберзахисту, що позитивно впливає на забезпечення ефективного моніторингу та аналізу стану безпеки, покращення реагування на кіберінциденти.

Залежно від призначення системи моніторингу подій перероблена та знову створена інформація відображається у зрозумілому для менеджменту безпеки вигляді, готується у вигляді стандартизованих звітів та використовується для належного реагування на кіберінциденти.

Системи SIEM відіграють ключову роль у забезпеченні безпеки корпоративних ІКС, що охоплюють велику кількість користувачів і технологічного обладнання, тому формування коректного та достатнього переліку вимог до створюваної та впроваджуваної системи має особливе значення.

Безумовно, вимоги до системи SIEM повинні враховувати конкретні потреби користувачів ІКС та менеджменту безпеки, а також особливості побудови та функціонування інформаційних технологій що використовуються .

Виходячи з необхідності дотримання політики інформаційної безпеки в частині забезпечення конфіденційності, цілісності та доступності інформації в ІКС уявляється доцільним сформулювати відповідні вимоги.

1. По аналогії радіотехнікою визначимо поняття чутливості та селективності виявлення аномалій за допомогою системи SIEM. Позначимо H_0, H_1 – гіпотези, які відповідають припущенню що ІКС перебуває в штатному стані та в стані виникнення (поширення) кіберінциденту відповідно.

Нехай $\alpha = P\left({}^{H_1}/_{H_0}\right)$ – умовна ймовірність відхилити вірну гіпотезу H_0. Значення α – будемо називати помилкою першого роду, яка характеризує помилкове спрацювання сигналу «тривоги» від системи. Занадто велике значення помилки першого роду буде призводити до зайвих витрат часу на опрацювання відповідних ситуацій та невиправданого відволікання організаційно-технічного ресурсу системи кіберзахисту. Воно фактично характеризує здатність SIEM відхиляти реально випадкові ситуації (інакше – забезпечувати селективність).

Далі позначимо $\beta = P\left({}^{H_0}/_{H_1}\right)$ – умовну ймовірність прийняти вірною гіпотезу H_0, хоча насправді вірна гіпотеза H_1 . Значення β – будемо називати помилкою другого роду, яка характеризує можливість що аномалії, причиною яких є кіберінциденти, будуть невиявлені. Зрозуміло, що ця характеристика саме нагадує про «чутливість» конкретної версії SIEM, вона пов'язана з ризиками втрати конфіденційності, цілісності та доступності інформаційних активів.

Таким чином, для забезпечення ефективної роботи SIEM необхідно мінімізувати відповідні ймовірності α, β.

2. Зважаючи на те, що після отримання вірного сигналу тривоги про початок кіберінцидента в системі захисту необхідно реалізувати низку контрзаходів $\{E_1, E_2, \dots, E_n\}$, які потребують певного часу на опрацювання $\{t_1, t_2, \dots, t_n\}$ необхідно, щоб час затримки Δt на формування сигналу тривоги був мінімізований $\Delta t \leq \min_j t_j$.

3. Для забезпечення ефективного управління інцидентами в SIEM має бути набір автоматизованих (за можливості, автоматичних) інструментів для виконання процедур відстеження, реагування на загрози та розслідування кіберінцидентів, зокрема шляхом інтеграції з іншими системами безпеки, наприклад, SOAR (Security Orchestration, Automation and Response).

4. Виходячи з засад політики Zero Trust (повної недовіри) в SIEM має бути реалізоване розмежування та контролю доступу до даних системи, а також забезпечення криптографічними методами контроля цілісності та конфіденційності інформаційних потоків та ресурсів, що виключатиме типові атаки типу «людина посередині» [12,13], «розділяй та керуй» тощо.

5. Зважаючи на постійний розвиток математичного апарату і технологій підтримки прийняття рішень, методів кореляційного аналізу даних, перспективи використання

машинного навчання для виявлення трендів і патернів [11] актуальною постачає задача відкритих інтерфейсів та протоколів інтеграції SIEM з зовнішніми застосунками.

Виходячи з загальних підходів до побудови автоматизованих систем доцільно звернути увагу на виконання наступних рекомендацій щодо SIEM:

−відповідність вимогам нормативно-правовим актам, міжнародним і національним стандартам (зокрема, PCI DSS, GDPR тощо);

−здатність до масштабування, що не впливатиме на безпеку застосування;

−максимальна підтримка інтеграції з джерелами даних, які здатні оперативно постачати достовірну інформацію з підтримкою надання даних як у реальному часі, так і пакетному режимі;

−спроможність зберігання великих масивів інформації що постійно зростають;

−підтримка кастомізації повідомлень, оповіщень і звітів.

5. Висновки та перспективи подальших досліджень

У роботі розглянуто проблеми і задачі формування вимог до архітектури і функцій систем моніторингу кібербезпеки, що має особливе значення з точки зору як проєктування систем LMS та SIEM нового покоління або вдосконалення вже існуючих, так і в плані проведення процедур оцінювання відповідності таких систем реальним потребам забезпечення кіберзахисту об’єктів критичної інфраструктури.

Розглянуті характеристики систем реагування на кіберінциденти утворюють підґрунтя для їх подальшого детального аналізу з метою формування кількісних показників якості та ефективності систем моніторингу. Зокрема це стосується механізмів і правил фільтрації, нормалізації, агрегації та фільтрації даних, що використовуються для підтримки процедур прийняття рішень щодо управління ситуаціями, які пов’язані з кіберінцидентами.

Заслуговує на увагу дослідження та обґрунтування криптографічних рішень для захисту конфіденційності та цілісності використовуваних даних та управління ключами в криптографічні підсистемі SIEM. Особливого значення це питання набуває в аспекті розв’язання завдань криміналістичної форензіки.

Окремим напрямом подальших досліджень, який викликає значний інтерес в плані підвищення ефективності систем моніторингу безпеки, становить задача побудови моделей машинного навчання з метою виявлення в досліджуваних вихідних даних трендів і патернів.

Список використаної літератури

1. Smirnova, T., Konstantynova, L., Konoplitska-Slobodeniuk, O., Kozlov, Y., Kravchuk, O., Kozirova, N., & Smirnov, O. (2024). Study of the Current State of SIEM Systems. Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(25), 6–18. https://doi.org/10.28925/2663-4023.2024.25.618

2. Accorsi, R. (2009). Log data as digital evidence: What secure logging protocols have to offer? 2009 33rd Annual IEEE International Computer Software and Applications Conference, 2, 398–403. doi:10.1109/COMPSAC.2009.166

3. Kusaka et al. (2014) Log Management System and Program. United States Patent US 8,738,625 B2. 47p.

4. Holik, F. et al. (2015) The deployment of security information and event management in cloud infrastructure. 25th International Conference Radioelektronika. 399-404. ISBN 978-1-4799-8117-5

5. Safarzadeh, M et al. (2019) A Novel and Comprehensive Evaluation Methodology for SIEM. Information Security Practice and Experience, ISPEC 2019 Vol. 1879. 476-488.

6. Gonzalez-Granadillo, G. (2021) Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. SENSORS. 21(14). AN 4759.

7. Gibert, D., Mateu, C., & Planes, J. (2020). The Rise of Machine Learning for Detection and Response: SIEM Evolution. ACM Computing Surveys, 53(4), 85-105. doi:10.1145/3409573

8. Chinenye Cordelia Nnamani (2024) Exploiting AI Capabilities: An in-Depth Analysis of Artificial Intelligence Integration in Cybersecurity for Threat Detection and Response. International Journal of Education, Management, and Technology. 2(3), 2024. 268-286.

9. Mohammad Habibullah Rakib et al. (2022) A Blockchain-Enabled Scalable Network Log Management System. Journal of Computer Science, 18 (6): 496.508 DOI:10.3844/jcssp.2022.496.508

10. Sheeraz, M (2023) Effective Security Monitoring Using Efficient SIEM Architecture. Human-Centric Computing and Information Sciences. Vol.13 AN 23. DOI:10.22967/HCIS.2023.13.023

11. Prathipa. A. R. (2024) Integrating Predictive Analytics with SIEM for Enhanced Threat Detection. Indian Journal of Information Technology. 4(1), 2024, 1-11. ISSN Online: 2251-2813

12. Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man in the Middle Attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027-2051. DOI:10.1109/COMST.2016.2548426

13. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). Information and cyber security of the enterprise. Textbook. Lviv: Publisher Marchenko T. V.

References

1. Smirnova, T., Konstantynova, L., Konoplitska-Slobodeniuk, O., Kozlov, Y., Kravchuk, O., Kozirova, N., & Smirnov, O. (2024). Study of the Current State of SIEM Systems. Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 1(25), 6–18. https://doi.org/10.28925/2663-4023.2024.25.618

2. Accorsi, R. (2009). Log data as digital evidence: What secure logging protocols have to offer? 2009 33rd Annual IEEE International Computer Software and Applications Conference, 2, 398–403. doi:10.1109/COMPSAC.2009.166

3. Kusaka et al. (2014) Log Management System and Program. United States Patent US 8,738,625 B2. 47 p.

4. Holik, F. et al. (2015) The deployment of security information and event management in cloud infrastructure. 25th International Conference Radioelektronika. 399-404. ISBN 978-1-4799-8117-5

5. Safarzadeh, M et al. (2019) A Novel and Comprehensive Evaluation Methodology for SIEM. Information Security Practice and Experience, ISPEC 2019 Vol. 1879. 476-488.

6. Gonzalez-Granadillo, G. (2021) Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. SENSORS. 21(14). AN 4759.

7. Gibert, D., Mateu, C., & Planes, J. (2020). The Rise of Machine Learning for Detection and Response: SIEM Evolution. ACM Computing Surveys, 53(4), 85-105. doi:10.1145/3409573

8. Chinenye Cordelia Nnamani (2024) Exploiting AI Capabilities: An in-Depth Analysis of Artificial Intelligence Integration in Cybersecurity for Threat Detection and Response. International Journal of Education, Management, and Technology. 2(3), 2024. 268-286.

9. Mohammad Habibullah Rakib et al. (2022) A Blockchain-Enabled Scalable Network Log Management System. Journal of Computer Science, 18 (6): 496.508 DOI:10.3844/jcssp.2022.496.508

10. Sheeraz, M (2023) Effective Security Monitoring Using Efficient SIEM Architecture. Human-Centric Computing and Information Sciences. Vol.13 AN 23. DOI:10.22967/HCIS.2023.13.023

11. Prathipa. A. R. (2024) Integrating Predictive Analytics with SIEM for Enhanced Threat Detection. Indian Journal of Information Technology. 4(1), 2024, 1-11. ISSN Online: 2251-2813

12. Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man in the Middle Ages. IEEE Communications Surveys & Tutorials, 18(3), 2027-2051. DOI:10.1109/COMST.2016.2548426

13. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). Information and cyber security of the enterprise. Textbook. Lviv: Publisher Marchenko T. V.