DOI 10.31891/2307-5732-2025-347-54
УДК 004.056:004.942

РИЖИЙ ЯРОСЛАВ
Хмельницький національний університет
e-mail: mirsvqwertyi@gmail.com
ЧЕШУН ВІКТОР
Хмельницький національний університет
https://orcid.org/0000-0002-3935-2068
e-mail: cheshunvn@khmnu.edu.ua
ЧЕШУН ОЛЕКСАНДР
Хмельницький національний університет
e-mail: Sashacn228@gmail.com
ЧЕШУН ДМИТРО
Хмельницький фаховий економіко-технологічний коледж УЕП
e-mail: dmitry_95@ukr.net

МОДЕЛЬ ТЕХНОЛОГІЇ ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ ОСОБОВИХ АТРИБУТІВ

Стаття присвячена презентації моделі технології синтезу сигнатури цифрового підпису на основі особових атрибутів. В роботі здійснено аналіз і класифікацію атрибутів підписанта для використання в сигнатурі цифрового підпису, визначено спосіб представлення і розподілу атрибутів в математичній моделі, презентована схема утворення сигнатури цифрового підпису в термінах математичної моделі. Сигнатура цифрового підпису, синтезована на основі двійкових векторів атрибутів, разом з хеш-сигнатурою відкритого тексту може піддаватися криптографічному шифруванню (закриттю) і додаватися до відкритого тексту за класичними технологіями накладання ЕЦП. Також можливе використання сигнатури цифрового підпису на основі атрибутів і у відкритому вигляді, без закриття шифруванням, що визначається цілями та потребами підписанта.

Ключові слова: захист інформації, електронний цифровий підпис, атрибути користувача, система електронного документообігу.

RYZHYI YAROSLAV, CHESHUN VIKTOR, CHESHUN OLEKSANDR
Khmelnytsky National University
CHESHUN DMYTRO
Khmelnytskyi Vocational Economic and Technological College of the UEE

MODEL OF DIGITAL SIGNATURE TECHNOLOGY BASED ON PERSONAL ATTRIBUTES

Abstract. The article is devoted to the presentation of a mathematical model of the digital signature synthesis technology based on personal attributes. The paper analyzes and classifies the attributes of the signatory for use in a digital signature, defines the method of presentation and distribution of attributes in a mathematical model. In the model of technology, sets of identifying, non-identifying and contextual attributes are defined. Each value of the attribute is a binary representation of the corresponding attribute, which allows you to identify the elements of the sets as binary codes or binary vectors of attributes and use methods of working with binary numbers.

To implement the technology, a scheme for generating signatures using elements of a mathematical model is proposed. The formation of a digital signature is reduced to the selection of elements of sets of identification, non-identification and contextual attributes that meet the needs or wishes of the signatory, and combining them into a single binary sequence - attribute-based digital signature (ABDS). A digital signature synthesized on the basis of binary attribute vectors, together with the plain text, can be subjected to cryptographic encryption (closing) and added to a packet with a hash signature using classic electronic digital signature technologies. It is also possible to use a digital signature ABDS attributes and in open form, without encryption, determined by the goals and needs of the signer. These two expected prospects make it possible to use the digital signature technology in electronic document management systems more widely, and the technology itself to be more flexible and more universal. The solutions are the basis of the algorithmic implementation of digital signature technology using attributes.

Keywords: information protection, electronic digital signature, user attributes, electronic document management system.

Вступ

Сучасний світ невпинно рухається у напрямку цифрової трансформації, змінюючи спосіб, яким ми працюємо і спілкуємося. У цьому контексті системи електронного документообігу стають ключовим інструментом для забезпечення ефективного обміну даними та документами між організаціями, установами та приватними особами [1]. Подібні системи є невід'ємною складовою сучасного підприємства чи організації, вони дозволяють значно зменшити витрати часу та ресурсів, пов'язаних з обробкою, зберіганням та передачею паперових документів. Вони сприяють автоматизації рутинних процесів, забезпечуючи швидкий доступ до необхідної інформації в будь-який час і в будь-якому місці. У зв'язку з розвитком роботи на віддалених робочих місцях, системи електронного документообігу дозволяють забезпечити ефективний обмін документами в реальному часі, незалежно від місцезнаходження користувачів. Це сприяє підвищенню продуктивності та зручності роботи, що є особливо важливим у сучасному глобалізованому світі.

Системи електронного документообігу також сприяють і поліпшенню безпеки даних [2]. Вони дозволяють керувати доступом до конфіденційної інформації, забезпечуючи шифрування даних та механізми перевірки цілісності. Це допомагає запобігти несанкціонованому доступу до важливих даних та зменшити ризик витоку інформації. Одним із основних інструментів кібербезпеки систем електронного документообігу є використання цифрових підписів [3].

Постановка задачі

Електронний цифровий підпис (ЕЦП) – це технологічний механізм, який дозволяє вам електронно підписувати документи або інші електронні повідомлення [4]. Ігнорування ЕЦП – одна з найбільш поширених слабких сторін систем електронного документообігу [3].

До недоліків традиційних технологій ЕЦП, що базуються на використанні криптографічних алгоритмів, можна віднести знеособлення підписанта і централізацію дій з підписом. Для формування, накладання і підтвердження ЕЦП підписант і верифікатор підпису повинні звертатися до послуг спеціалізованих сервісів високої довіри і не мають змоги ні сформувати ЕЦП власноруч, ні отримати з нього інформацію про підписанта.

Альтернативним напрямком розвитку технологій цифрового підпису є формування підпису на основі атрибутів підписанта, що робить підпис безпосередньо інформаційно пов'язаним з особою його надавача і максимально інформативним для верифікатора підпису, а самого підписанта перетворює у автора і власника підпису, як це є при використанні власноручного підпису.

Поняття підписів із застосуванням атрибутів було явно введено науковцями з Китаю в роботі [6], а Hemanta K Maji з співавторами [7] продовжив цю роботу і описує підпис із застосуванням атрибутів як «універсальний примітив, що дозволяє стороні підписувати повідомлення з детальним контролем над ідентифікаційною інформацією».

Існуючий, але в основному теоретичний проєкт під назвою ABCJTrust [8] мав на меті розробити структуру під ідентифікатором ABC (Attribute-based Credentials – облікові дані на основі атрибутів) на основі існуючої технології використання атрибутів в системах електронного документообіг.

Подібним, але більш практичним проєктом є Yivi [9] – технологія, спрямована на реалізацію функціонального потенціалу облікових даних на основі атрибутів. Для впровадження облікових даних із застосуванням атрибутів Yivi (частково) покладається на систему ідентифікації Identity Mixer (Idemix), розроблену IBM Research [10]. Система IBM Idemix надає різні функціональні можливості для підтвердження володіння обліковими даними із застосуванням атрибутів та їхніми властивостями.

Важливим аспектом технології використання цифрового підпису із застосуванням атрибутів в є мінімізація і актуалізація даних, коли йдеться про забезпечення конфіденційності користувачів. Це вимагається законодавством України [11] і ЄС [12]. Проте, мінімізація даних може призвести до зниження рівня інформаційної цінності цих даних. Коли розкривається менше даних, отримувач (верифікатор) може мати менше актуальної йому інформації. Слід розглянути баланс між збереженням високої інформаційної цінності виявлених даних і їх мінімальних розкриттям.

Для досягнення балансу між розкриттям і забезпеченням конфіденційності особових атрибутів у цифровому підписі виникає потреба визначення математичного апарату для формалізації даних і процесів їх обробки при формуванні підпису, а також розробки технології формування сигнатури атрибутивного цифрового підпису в термінах математичної моделі.

Основна частина

У випадку цифрових підписів є потреба розкривати не занадто багато особистої інформації про підписанта, але розкрита інформація повинна бути достатньо інформативною та зрозумілою. Це потребує аналізу і класифікації атрибутів, які можуть бути використані при формуванні сигнатури атрибутивного підпису.

Проведений аналіз дозволив виділити три типових категорії атрибутів особи:

- ідентифікаційні атрибути;
- неідентифікаційні атрибути;
- контекстуальні атрибути.

Ідентифікаційні атрибути однозначно дозволяють ідентифікувати особу без додаткових уточнень.

До ідентифікаційних атрибутів відносяться: відбиток пальця; малюнок сітківки ока; ПІБ; підпис особи (рукописний); ідентифікаційний код; серія-номер паспорта; серія-номер диплома; офіційний псевдонім (псевдонім, який однозначно пов'язаний з особою); ідентифікатор (номер або серія-номер) посвідчення з місця роботи тощо.

Як неідентифікаційні атрибути визначено такі дані особи, які в певному аспекті ідентифікують особу, але не дозволяють однозначно її ідентифікувати без додаткових уточнень, оскільки можуть належати певному колу осіб або мають масове розповсюдження. До неідентифікаційних атрибутів можна віднести: ім'я; по батькові; розповсюджене прізвище; освіту; фах; місце роботи; посаду; неідентифікуючий особу псевдонім (широко розповсюджений або такий, що відомий тільки довіреній особі або обмеженому колу довірених осіб); дата народження; вік; дата видачі паспорту (будь-якого іншого документа тощо); орган, що видав паспорт (будь-який інший документ тощо) та інші.

Якщо ідентифікаційні атрибути служать для точної ідентифікації особи, то неідентифікаційні атрибути особисту інформацію без прямої ідентифікації.

Як контекстуальні атрибути підпису розглядаємо такі характеристики або ж параметри, які визначаються або можуть змінюватися залежно від конкретного контексту чи поточних обставин. В контексті ідентифікації особи ці атрибути надають додаткову інформацію про користувача, яка може бути корисною для точнішої та надійнішої ідентифікації підписанта в певному середовищі чи ситуації.

До контекстуальних атрибутів можна віднести: часові параметри накладання ЕЦП (дата, час, день тижня, місяць тощо); геолокаційні параметри накладання ЕЦП (геолокаційні координати, адреса або складові адреси, установа або офіс з можливістю уточнення їх місцезнаходження тощо); тип пристрою, задіяного для накладання цифрового підпису; дані автентифікації під час входу в систему; права та повноваження підписанта; роль підписанта у певному контексті тощо.

При визначенні базових принципів увага акцентується на забезпеченні гнучкості, адаптивності та мультиатрибутності ЕЦП. Зазначені принципи передбачають надання підписанту можливості формувати цифровий підпис з довільної кількості атрибутів та визначати їх склад за власним побажанням або у відповідності до потреб.

Для гнучкості процедур автоматизованого вибору атрибутів і забезпечення математичного підґрунтя адаптивності мультиатрибутного формування ЕЦП формуються множини відповідних атрибутів:

– IA:{IA_1, IA_2, … , IA_i, … , IA_k} – множина ідентифікаційних атрибутів (Identifying Attributes) особи-підписанта;

– NIA:{NIA_1, NIA_2, … , NIA_j, … , NIA_m} – множина неідентифікаційних атрибутів (Non-Identifying Attributes) особи-підписанта;

– CA:{CA_1, CA_2, … , CA_l, … , CA_n} – множина контекстуальних атрибутів (Contextual Attributes) особи-підписанта або самого підпису.

Схема формування цифрового підпису в примітивах математичної моделі представлена на рисунку 1.

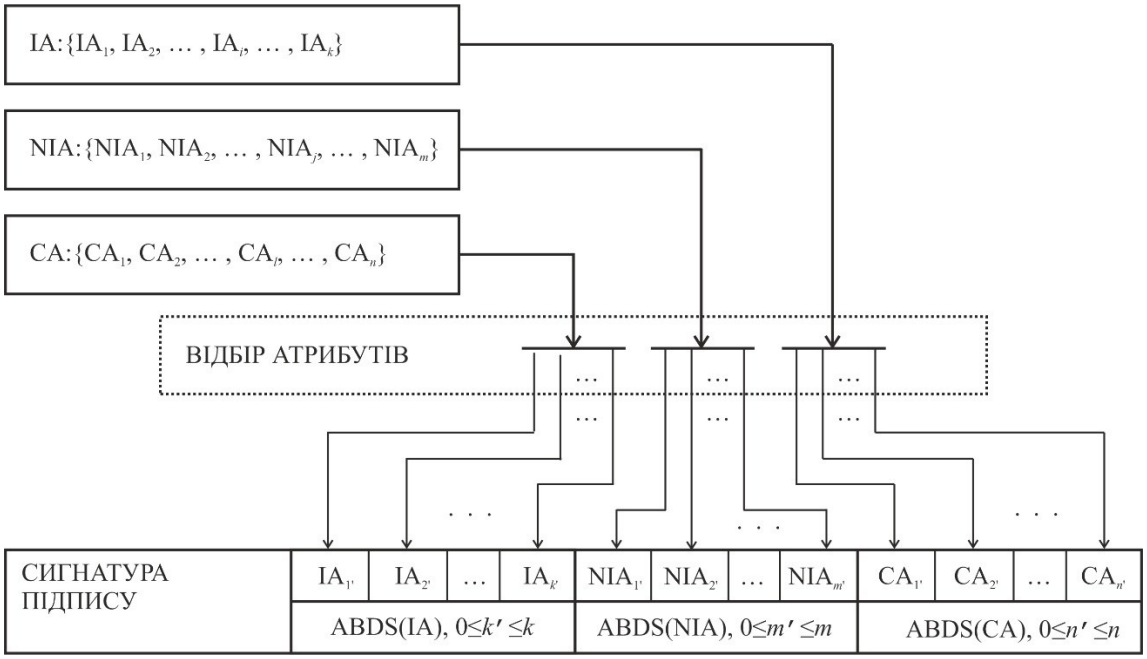

Рис. 1 – Схема утворення сигнатури цифрового підпису з атрибутів

Кожне значення атрибуту $IA_i \in IA$, $NIA_j \in NIA$ і $CA_l \in CA$ є двійковим представленням відповідного атрибуту, що дозволяє ідентифікувати елементи множин як двійкові коди або двійкові вектори атрибутів. Формування цифрового підпису зводиться до вибору елементів множин $IA_i \in IA$, $NIA_j \in NIA$ і $CA_l \in CA$, які відповідають потребам-побажанням підписанта, та поєднання їх у єдину двійкову послідовність – вектор (сигнатуру) цифрового підпису на основі атрибутів ABDS (Attribute-Based Digital Signature).

Наведені на схемі для полів ABDS(IA), ABDS(NIA), ABDS(CA) обмеження $0 \le k' \le k$, $0 \le m' \le m$, $0 \le n' \le n$ ілюструють, що в ході утворення сигнатури цифрового підпису ABDS до її складу можуть включатися атрибути кожного класу у будь-якій кількості від нуля (атрибути відповідного класу і саме поле цих атрибутів в сигнатурі цифрового підпису будуть відсутні) до максимальної кількості задекларованих атрибутів.

Висновки

В статті розглянута модель технології цифрового підпису із використанням атрибутів підписанта та презентована схема утворення сигнатури цифрового підпису в термінах математичної моделі. Сигнатура ABDS цифрового підпису, синтезована на основі двійкових векторів атрибутів, разом з файлом відкритого тексту, може піддаватися криптографічному шифруванню (закриттю) і з хеш-сигнатурою додаватися до відкритого тексту за класичними технологіями накладання ЕЦП. В той же час, можливе використання сигнатури цифрового підпису на основі атрибутів ABDS і у відкритому вигляді, без закриття шифруванням, що визначається цілями та потребами підписанта. Ці дві передбачувані

перспективи роблять можливим використання технології цифрового підпису в системах електронного документообігу більш широкими, а саму технології гнучкішою і більш універсальною.

Література

1. Асанова, Л. (2021). Місце електронного документообігу в загальній системі діловодства. *Адміністративне право і процес, 3*, 156–160.
2. Севастєєв, Є. О. (2022). *Безпека електронного документообігу*. Одеса: ДУІТЗ.
3. Rauniyar, K. (2021). Role of FinTech and innovations for improvising digital financial inclusion. *International Journal of Innovative Science and Research Technology, 6*, 1419–1424.
4. Електронний підпис і сертифікація документів. (н.д.). Отримано 27 листопада 2023 з https://pidru4niki.com/19590809/informatika/elektronniy_pidpis_sertifikatsiya_dokumentiv
5. Політанський, В. С. (2021). Теоретико-правові засади системи електронного документообігу в Україні. *Право і суспільство, 1*, 22–27.
6. Guo, S., & Zeng, Y. (2008). Attribute-based signature scheme. In *2008 International Conference on Information Security and Assurance (ISA 2008)* (pp. 509–511). IEEE.
7. Maji, H. K., Prabhakaran, M., & Rosulek, M. (2011). Attribute-based signatures. In *Cryptographers' Track at the RSA Conference* (pp. 376–392). Springer.
8. ABC4Trust. (н.д.). *Attribute-based Credentials for Trust*. Отримано 28 листопада 2023 з https://abc4trust.eu/download/ABC4Trust-OnePager-About-ABC4Trust.pdf
9. Yivi. (н.д.). *How Yivi works?* Отримано 28 листопада 2023 з https://www.yivi.app/en/for-me/how-yivi-works
10. Bringer, A., Gordon, C., Mackey, S., & Smith, R. (н.д.). *Idemix: Identity Mixer*. Отримано 29 листопада 2023 з https://faculty.uca.edu/ronmc/INFO3321/Spring_2007/ET%20Pres/ET1/G4/Idemix%20Group%204.htm
11. Верховна Рада України. (2022). *Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 01.12.2022 р.* Отримано 29 листопада 2023 з https://zakon.rada.gov.ua/laws/show/2155-19/ed20231231#Text
12. European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union*, 4.5.2016, 88 p.

References

1. Asanova, L. (2021). Mistse elektronnoho dokumentoobihu v zahalnii systemi dilovodstva. Administratyvne pravo i protses, 3, 156–160.
2. Sevastieiev, Ye. O. (2022). Bezpeka elektronnoho dokumentoobihu. Odesa: DUITZ.
3. Rauniyar, K. (2021). Role of FinTech and innovations for improvising digital financial inclusion. International Journal of Innovative Science and Research Technology, 6, 1419–1424.
4. Elektronnyi pidpys i sertyfikatsiia dokumentiv. (n.d.). Otrymano 27 lystopada 2023 z https://pidru4niki.com/19590809/informatika/elektronniy_pidpis_sertifikatsiya_dokumentiv
5. Politanskyi, V. S. (2021). Teoretyko-pravovi zasady systemy elektronnoho dokumentoobihu v Ukraini. Pravo i suspilstvo, 1, 22–27.
6. Guo, S., & Zeng, Y. (2008). Attribute-based signature scheme. In 2008 International Conference on Information Security and Assurance (ISA 2008) (pp. 509–511). IEEE.
7. Maji, H. K., Prabhakaran, M., & Rosulek, M. (2011). Attribute-based signatures. In Cryptographers' Track at the RSA Conference (pp. 376–392). Springer.
8. ABC4Trust. (n.d.). Attribute-based Credentials for Trust. Otrymano 28 lystopada 2023 z https://abc4trust.eu/download/ABC4Trust-OnePager-About-ABC4Trust.pdf
9. Yivi. (n.d.). How Yivi works? Otrymano 28 lystopada 2023 z https://www.yivi.app/en/for-me/how-yivi-works
10. Bringer, A., Gordon, C., Mackey, S., & Smith, R. (n.d.). Idemix: Identity Mixer. Otrymano 29 lystopada 2023 z https://faculty.uca.edu/ronmc/INFO3321/Spring_2007/ET%20Pres/ET1/G4/Idemix%20Group%204.htm
11. Verkhovna Rada Ukrainy. (2022). Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy: Zakon Ukrainy vid 01.12.2022 r. Otrymano 29 lystopada 2023 z https://zakon.rada.gov.ua/laws/show/2155-19/ed20231231#Text
12. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, 4.5.2016, 88 p.

DOI 10.31891/2307-5732-2025-347-55
УДК 004.056:004.942

МАЛИЦЬКИЙ ТАРАС
Хмельницький національний університет
e-mail: tarasmalitskyi@gmail.com
ЧЕШУН ВІКТОР
Хмельницький національний університет
https://orcid.org/0000-0002-3935-2068
e-mail: cheshunvn@khmnu.edu.ua
ОЛЕКСЮК ДМИТРО
Хмельницький фаховий економіко-технологічний коледж УЕП
https://orcid.org/0009-0006-3735-1930
e-mail: oleksuk.dima@gmail.com
ЧЕШУН ДМИТРО
Хмельницький фаховий економіко-технологічний коледж УЕП
e-mail: dmitry_95@ukr.net

МАТЕМАТИЧНА МОДЕЛЬ МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ ІМОВІРНІСНИХ КРИТЕРІЇВ ДОВІРИ

Стаття присвячена презентації математичної моделі методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу із застосуванням імовірнісних критеріїв довіри. За результатами аналізу покладених на метод завдань, концептуально математичну модель методу захисту інформаційних ресурсів корпоративної мережі класифіковано як ймовірнісну статистичну модель систем управління доступом на основі концепції (критеріїв) довіри. Математична модель методу базується на аналізі взаємодії між різними суб'єктами (користувачами) та об'єктами (інформаційними ресурсами) в інформаційному середовищі корпоративної мережі та дає інструментарій для визначення ступеня довіри до суб'єктів інформаційних відносин в корпоративній мережі з точки зору інформаційної безпеки. Принципи застосування моделі продемонстровано структурно-логічною схемою взаємозв'язку елементів математичної моделі в реалізації методу.

Ключові слова: захист інформації, контроль доступу, корпоративна мережа, критерії довіри.

MALYTSKYI TARAS, CHESHUN VIKTOR
Khmelnytsky National University
OLEKSIUK DMYTRO, CHESHUN DMYTRO
Khmelnytskyi Vocational Economic and Technological College of the UEE

MATHEMATICAL MODEL OF THE METHOD OF PROTECTING CORPORATE NETWORK INFORMATION RESOURCES USING PROBABILITY TRUST CRITERIA

Abstract. The article is devoted to the presentation of a mathematical model of the method of protecting information resources of the corporate network from unauthorized access using probabilistic trust criteria. According to the results of the analysis of the tasks assigned to the method, the conceptual mathematical model of the method of protecting information resources of the corporate network is classified as a probabilistic statistical model of access control systems based on the concept (criteria) of trust. The mathematical model of the method is focused on the statistical analysis of the interaction between various subjects (users) and objects (information resources) in the information environment of the corporate network and provides a toolkit for determining the degree of trust in subjects of information relations in the corporate network from the point of view of information security.

Plural of objects and subjects of information relations are identified in the model. A binary access matrix was selected as the main element for managing access to information resources of the corporate network, the rules for its formation are detailed. A formula for calculating the probabilistic criterion of trust in the user based on statistical data about his actions in the network is also proposed. The principles of using the data of the vector of trust criteria and the vector of limit restrictions for making changes to the user's access rights are defined. The change of access rights is implemented in real time through the adjustment of the access matrix taking into account the decrease in the criterion of trust in the user according to the statistics of his work.

The principles of applying the model are demonstrated by the structural and logical diagram of the relationship between the elements of the mathematical model in the implementation of the method.

Keywords: information protection, access control, corporate network, trust criteria.

Вступ

Поширення цифрових технологій та нарощування їх можливостей супроводжується одночасним збільшенням кількості кіберзагроз. За таких умов ключовим аспектом сучасного бізнесу стає безпека корпоративних мереж як основної інфраструктури для забезпечення зв'язку і ефективної взаємодії між всіма рівнями організації, а також головного сховища комерційної та конфіденційної інформації.

Забезпечення ефективної безпеки корпоративних мереж вимагає комплексного підходу, який охоплює технологічні інновації та докладний аналіз потенційних загроз [1]. Технологічні інновації включають організаційні та програмно-апаратні заходи безпеки, такі як міжмережеві екрани, антивірусне програмне забезпечення, шифрування даних, аутентифікація та авторизація, навчання персоналу, регулярні оновлення та патчі, резервне копіювання та відновлення даних, а також моніторинг та аналіз активності мережі.

Одним із головних аспектів інформаційної безпеки корпоративних мереж є саме постійний моніторинг та аналіз активності мережі для блокування потенційно можливих шкідливих дій з інформаційними ресурсами [2]. Систематичний моніторинг мережі та виявлення загроз дозволяють не лише своєчасно реагувати на кібератаки та аномальну активність, але і запобігати можливим інцидентам кібербезпеки.