УДК 004.75
DOI https://doi.org/10.32782/2663-5941/2025.6.2/36

Олійник П.А.
Хмельницький національний університет

Савенко О.С.
Хмельницький національний університет

Гнатюк О.І.
Національна академія державної прикордонної
служби України імені Богдана Хмельницького

КОНЦЕПТУАЛЬНА АРХІТЕКТУРА СИСТЕМИ ДЛЯ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ У КОРПОРАТИВНИХ МЕРЕЖАХ

У статті розглянуто актуальну проблему оцінювання стану захищеності даних корпоративних систем у контексті зростання складності розподілених корпоративних мереж та підвищених вимог до їхньої надійності та стійкості. Проведено аналіз сучасних наукових досліджень і комерційних рішень у сфері моніторингу, управління та аналітики кібербезпеки в результаті якого виявлено низку обмежень. Зокрема, більшість існуючих підходів орієнтовані на виявлення інцидентів або моніторинг подій, однак не забезпечують комплексної кількісної оцінки рівня захищеності інформаційних ресурсів на основі стандартизованих показників. Також, у таких систем відсутні механізми побудовані на основі штучного інтелекту та машинного навчання, що дозволяли б робити прогнозовані оцінки та моделювати динаміку змін стану безпеки у часі. Крім того, у сучасних системах відсутній фокус на розроблені механізмів гнучкої координації взаємодії між елементами розподіленого середовища, що може призводити до надмірного навантаження на центральні вузли, зниження ефективності обміну даними та втрати стабільності у разі виникнення відмов або змін у мережевій топології.

З метою усунення виявлених недоліків запропоновано концептуальну архітектуру агентно-орієнтованої розподіленої системи з елементами динамічної централізації, яка забезпечує автоматизоване оцінювання стану інформаційної безпеки у корпоративних середовищах та не потребує залучення системних адміністраторів під час її функціонування. У запропонованій системі програмні агенти встановлюються на вузлах корпоративної мережі та здійснюють оцінювання поточного рівня захищеності даних на основі формалізованих показників, які узгоджені із міжнародними стандартами кібербезпеки. Взаємодія між агентами організована за принципом динамічної централізації, що дозволяє адаптивно змінювати роль лідера, забезпечуючи високу відмовостійкість і збалансоване навантаження в системі. Централізований вузол в архітектурі системи виконує функції аналітичного та прогнозного центру, який дозволяє не лише узагальнювати результати оцінювання, а й передбачати тенденції зміни рівня безпеки в часі.

Проведено експеримент для виявлення ефективності роботи системи у різних сценаріях функціонування, що спрямований на перевірку стабільності, надійності та ефективності її архітектури. Оцінювання здійснювалося за рядом системних метрик, що відображають рівень доступності, відмовостійкості, затримку координації та комунікаційні витрати. Результати експерименту підтвердили доцільність використання агентно-орієнтованого підходу для побудови розподілених систем оцінювання інформаційної безпеки.

Ключові слова: *агентно-орієнтована система, корпоративна мережа, розподілені системи, динамічна централізація, програмний агент, оцінка інформаційної безпеки, NIST SP 800-53, ISO/IEC 27001:2022, ISO/IEC 27002:2022.*

Постановка проблеми. В останні роки інтернет став невід'ємною частиною повсякденного життя в усьому світі, але з іншого боку також зросла інтенсивність кібератак [1, с. 520]. Оскільки важливість кібербезпеки зростає в усіх галузях та на кожному організаційному рівні для протидії сучасним небезпекам і загрозам, корпоративна безпека стала невід'ємним елементом

сучасного світу [18, с. 2]. Корпоративні мережеві середовища обробляють велику кількість різноманітних персональних даних користувачів і складаються з широкого спектру взаємопов'язаних обчислювальних вузлів, включаючи персональні комп'ютери, ноутбуки та сервери. Зловмисники намагаються проникнути в мережеві середовища великих підприємств, щоб отримати доступ до приватної інформації користувачів або вивести з ладу певне мережеве обладнання і саме тому оцінка захищеності даних має вирішальне значення для забезпечення належного захисту критично важливих даних від несанкціонованого доступу [2, с. 293]. Виходячи з цього, сучасне цифрове середовище вимагає від організацій приділяти першочергову увагу захисту інформаційних активів і саме тому забезпечення конфіденційності, цілісності та доступності (КЦД) інформації стає фундаментальною передумовою не лише для відповідності регуляторним нормам, але й гарантує надійність зберігання даних [7, с. 1].

Для боротьби із постійно зростаючою кількістю кіберзагроз, що мають на меті отримати доступ до захищених даних підприємств, поточні дослідження зосередились на розробці автоматизованих, модульних та інтелектуальних систем, які здатні виконувати безперервні та автономні процеси моніторингу та реагування на кібератаки в мережевих середовищах. У цій статті пропонується концептуальна архітектура системи, призначеної для оцінки безпеки даних та інформації в корпоративних мережах. Запропонована архітектура поєднує розподілену автономію агентів з адаптивною централізованою координацією для підвищення надійності, масштабованості та відмовостійкості під час проведення процесу оцінювання захищеності.

Аналіз останніх досліджень і публікацій. Нещодавні дослідження підкреслюють зростаючу актуальність розподілених архітектур у покращенні виявлення шкідливих програм у корпоративних мережах. У [4, с, 266] представлено гібридний підхід в якому локальні вузли оцінюють певні показники безпеки та передають результати до центрального блоку для скоординованого прийняття рішень. Продовжуючи цю концепцію, робота [8, с. 407] представляє архітектуру, яка поєднує самоорганізацію та адаптивність з частковою централізацією. Використовуючи математичні моделі для визначення ключових показників, система ефективно балансує децентралізоване виявлення з централізованим керуванням. У [15, с. 125] пропонується графотеоретичний підхід для аналізу взаємодії вузлів та структури системи, який може підтримувати проектування масштабованих систем на основі агентів. У роботі [24, с. 263] розглянуто систему моніторингу розподілених мереж на основі граничних обчислень, що орієнтована на високу надійність і відмовостійкість. Архітектура передбачає три взаємопов'язані компоненти: збір даних, аналіз і локалізацію відмов. Вони взаємодіють через проміжний рівень контролера сервісних інтерфейсів. Такий підхід забезпечує ефективне управління інформаційними потоками між вузлами, знижуючи затримки та підвищуючи оперативність виявлення збоїв у великих мережах.

Система InDepth [3, с. 1974] усуває обмеження традиційного мережевого моніторингу, пропонуючи масштабовану та симетричну архітектуру для розподіленого збору даних. У статті [6, с. 362] представлено високопродуктивну систему моніторингу мережевого трафіку та виявлення вторгнень, яка реалізована на основі технології P4 для середовищ із високими вимогами до пропускної здатності та затримок. Рішення використовує вбудований підхід до аналізу трафіку, що забезпечує мінімальні затримки та високу точність виявлення атак. Дослідження демонструє ефективність інтеграції механізмів аналізу безпосередньо у мережеву інфраструктуру, підвищуючи масштабованість і надійність систем безпеки. Запропонований підхід є релевантним для розробки розподілених систем оцінювання стану захищеності інформації, де важливо забезпечити локальну обробку даних та ефективну координацію між вузлами. Комплексна архітектура систем моніторингу безпеки розглядається у роботі [16, с. 5], де запропоновано модульну структуру системи керування інформацією та подіями безпеки (SIEM), що забезпечує цілісне спостереження за станом інформаційної безпеки організації. Розподілення функціональності на окремі модулі підвищує гнучкість, спрощує масштабування та сприяє ефективнішій інтеграції з іншими підсистемами кіберзахисту. Такий підхід дозволяє організаціям формувати більш адаптивну архітектуру центрів безпеки (SOC) з можливістю розширення функціоналу без втрати продуктивності. Подальший розвиток ідеї комплексного контролю безпеки відображено у дослідженні [19, с. 681] в якому інтегровано SIEM-платформу з системою керування станом безпеки хмарного середовища (CSPM) для забезпечення автоматизованого аудиту відповідності нормативним вимогам GDPR і PDP. Запропонована інтеграція дозволяє не лише виявляти порушення політик безпеки,

а й формувати автоматичні звіти та здійснювати моніторинг конфігурацій хмарних сервісів у режимі реального часу.

Автономна система збору системних журналів на основі Kubernetes для малих та середніх підприємств (SMEs), яка підкреслює масштабованість, самостійне керування та відмовостійкість відображає сучасні тенденції в децентралізованих та модульних архітектурах для моніторингу корпоративного рівня [9, с. 36]. Було досліджено еволюцію від традиційного мережевого моніторингу до багатоагентних систем, які покращені генеративним штучним інтелектом для інтелектуального спільного виявлення загроз [12, с. 116]. Системи розширеного виявлення та реагування нового покоління демонструє рішення ZADIG [22, с. 690], що відноситься до класу систем розширеного виявлення та реагування (XDR), в якому використано штучний інтелект і машинне навчання для прогнозування повторних аномалій та зниження кількості хибних спрацьовувань. Модульна архітектура системи забезпечує високу масштабованість, а спеціалізований механізм оброблення даних гарантує ефективну агрегацію потоків з різних джерел. Експериментальні результати довели здатність системи ефективно виявляти складні атаки, такі як «людина посередині» та DDoS-впливи. У роботі [25, с. 1] розглянуто підходи до підвищення ефективності систем моніторингу безпеки шляхом інтеграції алгоритмів машинного навчання у традиційні рішення типу SIEM. Сучасні системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) генерують значний обсяг попереджень та потребують постійного оновлення сигнатур, що знижує їхню ефективність у виявленні нових типів атак. Запропоновано метод виявлення аномалій на основі машинного навчання, який дозволяє автоматично класифікувати мережевий трафік і підвищити точність виявлення кіберінцидентів. Запропонований підхід спрямований на зменшення кількості хибнопозитивних спрацювань і покращення здатності SIEM-систем до аналізу великих обсягів даних, що надходять із мережевої інфраструктури. Рішення IntelliWatch SIEM [23, с. 211] спрямоване на протидію нульовим дням і прихованим шкідливим програмам. Платформа об'єднує механізми збору, кореляції та реагування на інциденти, забезпечуючи безперервний моніторинг та автоматизовану обробку подій. Інтерфейс системи орієнтований на оперативність дій аналітиків, а реалізована інтеграція процесів виявлення, звітності та аудиту формує цілісний підхід до управління інформаційною безпекою.

Окрім розглянутих наукових досліджень, сучасна кібербезпека підприємств все ще значною мірою залежить від складних комерційних платформ, які інтегрують безперервний моніторинг, аналітику даних та механізми автоматизованого реагування. Одним із таких прикладів є рішення Symantec Endpoint Security Complete [20], що виступає комплексною системою виявлення та реагування на інциденти безпеки на кінцевих точках (EDR) система захисту кінцевих точок, розроблена компанією Broadcom, яка поєднує інструменти для запобігання, виявлення, аналізу та реагування на кіберзагрози. Архітектура платформи базується на інтеграції локальних агентів із централізованим хмарним середовищем, що забезпечує безперервну кореляцію подій та уніфіковане управління. Symantec використовує багаторівневу модель аналізу, яка включає статичне сканування, динамічну емуляцію, поведінковий моніторинг і машинне навчання для визначення складних загроз. Платформа підтримує концепцію Zero Trust, реалізуючи контроль доступу на основі ризику й поведінкової ідентифікації користувачів.

SentinelOne Singularity [5] позиціонується як платформа для автономної безпеки кінцевих точок та поєднує компоненти EDR та XDR систем. Його інтелектуальні агенти функціонують незалежно, що дозволяє проводити поведінковий аналіз у режимі реального часу безпосередньо на окремих пристроях. Ключова перевага цієї архітектури полягає в її локальній автономії, що зменшує час реакції та знижує залежність від централізованого моніторингу. SentinelOne використовує єдину базу телеметрії, що об'єднує дані з усіх кінцевих вузлів для формування цілісного уявлення про стан корпоративної безпеки. Інтерфейс консолі дозволяє адміністраторам швидко реагувати на інциденти, отримуючи контекст події та можливість автоматичного реагування. Така архітектура зменшує навантаження на центральні ресурси, підвищує відмовостійкість та забезпечує баланс між локальною автономністю і централізованим контролем.

Одним із найяскравіших прикладів сучасного захисту підприємств є CrowdStrike Falcon [17], яке містить елементи EDR та XDR систем. Це хмарна платформа для розширеного виявлення та реагування. Воно використовує програмних агентів, що розгортаються на кінцевих точках, які постійно спостерігають за поведінкою системи, виявляють аномалії та співвідносять події за допомогою

централізованої аналітики. Рішення інтегрується з іншими корпоративними інструментами безпеки, що дозволяє автоматизувати процеси реагування та скоротити час ліквідації загроз. Falcon демонструє високий рівень масштабованості, забезпечуючи централізований моніторинг без зниження продуктивності навіть у великих розподілених мережах.

ESET PROTECT Enterprise [11] є корпоративною платформою класу XDR для багаторівневого захисту, що об'єднує антивірусні механізми, поведінковий аналіз, управління вразливостями та інструменти для централізованого моніторингу Її архітектура побудована на агентній моделі, де агенти встановлюються на вузлах корпоративної мережі для збору телеметрії, моніторингу процесів і виявлення загроз. Всі дані передаються до консолі ESET PROTECT, яка виступає в ролі центрального аналітичного вузла. Інтеграція з модулем ESET Inspect забезпечує детальний аналіз подій, виявлення відхилень від нормальної поведінки системи та формування рекомендацій для реагування. Додатково платформа включає модулі керування оновленнями, аудит патчів, звітність відповідно до стандартів безпеки та підтримку політик доступу. Система забезпечує автоматичні та ручні сценарії реагування, дозволяючи адміністраторам балансувати між гнучкістю керування й автономністю агентів. Завдяки стабільності, простоті розгортання та можливості масштабування ESET PROTECT Enterprise є ефективним рішенням для великих корпоративних мереж із високими вимогами до стабільності та звітності.

Splunk Enterprise Security [21] належить до окремої категорії SIEM платформ, орієнтованих на управління інформацією та подіями безпеки. Платформа агрегує великі обсяги телеметрії з широкого кола систем та пристроїв, що дозволяє здійснювати комплексну кореляцію подій, розпізнавання шаблонів загроз та візуальну аналітику. Його перевага полягає в потужних аналітичних та конфігураційних можливостях, які дозволяють гнучко інтегруватися з різноманітними джерелами даних. Splunk служить центральним аналітичним рівнем у багатьох гібридних архітектурах безпеки, надаючи цінну інформацію для прийняття рішень та коригування політик.

Як наукові дослідження, так і комерційні інструменти демонструють значний прогрес у сфері моніторингу, автоматизації та аналітики кібербезпеки, однак вони приділяють обмежену увагу до комплексної оцінки інформаційної безпеки. Більшість існуючих рішень надають пріоритет виявленню та реагуванню на інциденти, але не мають механізмів для оцінки поточного стану інформаційної безпеки за допомогою математично формалізованих кількісних показників та метрик. Відсутність єдиного стандартизованого підходу до кількісної оцінки стану інформаційної захищеності не дозволяє повною мірою врахувати показники, які узгоджені з міжнародними стандартами кібербезпеки, що в свою чергу значно ускладнює інтеграцію таких оцінок у процеси комплексного аудиту та управління ризиками на рівні корпоративних підприємств.

Ще однією виявленою прогалиною є відсутність прогнозних механізмів, що здатні моделювати динаміку зміни стану безпеки у часі. Хоча багато систем уже застосовують методи штучного інтелекту або машинного навчання, проте у них відсутні механізми для проведення передбачень деградації рівня захищеності на основі попередньо накопичених історичних даних.

Крім того, зі зростанням складності розподілених систем кібербезпеки, завдання забезпечення високого рівня доступності, надійності та відмовостійкості в їхніх архітектурах стало важливим завданням, яке потребує подальшого вивчення та вдосконалення. Вкрай важливо постійно підвищувати ефективність координації в усіх елементах розподілених систем, щоб забезпечити їм ефективний режим функціонування та збалансований розподіл робочого навантаження за різних умов експлуатації.

Отже, існує потреба у створенні нового типу розподілених систем, які б поєднували автономний моніторинг, формалізоване оцінювання стану інформаційної безпеки та прогнозування її майбутніх змін, забезпечуючи при цьому високу надійність роботи та адаптивність до умов середовища функціонування.

Постановка завдання. Метою цієї роботи є представлення та обґрунтування концептуальної архітектури розподіленої агентно-орієнтованої системи з елементами динамічної централізації призначеної для оцінки захищеності даних та інформації в корпоративних мережах, а також подання опису її основних компонентів, операційних механізмів та комунікаційних каналів.

Виклад основного матеріалу. Відповідно до виявлених прогалин в існуючих рішеннях та підходах кібербезпеки призначених для великих корпоративних середовищ, у цій роботі пропонується концептуальна архітектура розподіленої агентно-орієнтованої системи з елементами динамічної централізації для оцінки стану інформаційної

безпеки в корпоративних мережах. В основі цієї архітектури лежать програмні агенти, які розгортаються на різних вузлах корпоративної мережі, включаючи робочі станції, ноутбуки, персональні комп'ютери (ПК) та сервери. Агенти функціонують незалежно один від одного та у повністю автономному режимі без будь-якої участі людини, виконуючи регулярні оцінки стану захищеноті даних поточного вузла. Така конструкція забезпечує розподілену роботу та забезпечує оперативне реагування в режимі реального часу на рівні вузла. Враховуючи це, поточну систему можна представити так:

$$S = \{(A_1, N_1), (A_2, N_2), (A_3, N_3), \ldots, (A_i, N_j)\}, \backslash^*$$

MERGEFORMAT (1)

де N_j – вузол мережі; A_i – програмний агент, який розгорнутий на конкретному вузлі мережі; $i = j = 1,2,3,...,n$; n – кількість вузлів мережі та програмних агентів.

В процесі функціонування системи, агенти спілкуючись один з одним, періодично беруть участь у процесах обрання найбільш сприятливого програмного компоненту для певного часового інтервалу. Цей механізм втілює принцип динамічної централізації в якому тимчасовий координуючий агент обирається не статично, а на основі періодичних оцінок показників навколишнього середовища вузла в якому він функціонує і тому має тенденцію змінюватись адаптуючись до умов постійно змінюваного стану корпоративної мережі. Така кількісна оцінка може включати різні критерії, такі як час безперебійної роботи та простою, завантаження процесора і оперативної пам'яті, температуру окремих апаратних елементів устаткування, а також інші показники надійності на рівні вузла. У кожному циклі оцінювання агент з найвищим показником навколишнього середовища обирається тимчасовим координатором, що відповідає за збір результатів оцінювання інформаційної безпеки від усіх інших агентів та пересилання результатів на віддалений персональний комп'ютер системного адміністратора. Це твердження можна представити наступною бінарною функцією:

$$\sum_{i=1}^{n} \delta_i(t) = 1, \delta_i(t) = \begin{cases} 1, i = c(t) \\ 0, i \neq c(t) \end{cases}, \backslash^* \text{ MERGEFORMAT (2)}$$

де $\delta_i(t)$ – бінарна функція для індикації координаційного статусу агента i в момент часу t; $i = j = 1,2,3,...,n$; n – кількість програмних агентів; $c(t)$ – індекс агента лідера.

Процес проведення виборів лідера здійснюється через автономну міжагентну комунікацію, що усуває необхідність у постійно централізованому блоці керування. У разі виходу узгоджувального програмного компоненту з ладу або зниження його надійності, агенти ініціюють процедуру виборів нового координатора. Цей процес відбувається автоматично та з мінімальними затримками у комунікації. Такий підхід допомагає уникнути перевантаження окремого вузла, підвищує відмовостійкість та покращує працездатність системи у разі раптових збоїв або цілеспрямованих атак, які впливають на ефективне функціонування окремих мережевих вузлів. Структура комунікації є динамічною та може бути подана у вигляді графа в якому агенти представляються вершинами, а зв'язки ребрами і має вигляд:

$$G(t) = (A, L(t)), \backslash^* \text{ MERGEFORMAT (3)}$$

де $G(t)$ – граф комунікації агентів i в момент часу t; $A = \{A_1, A_2, A_3, ..., A_n\}$; A – множина програмних агентів; $L(t) = \{(A_i, A_j) \# A_{ij}(t) = 1, i \neq j\}$; $L(t)$ – множина комунікаційних зв'язків; $A_{ij} = \begin{cases} 1, A_i \text{ і } A_j \text{ зв'язані} \\ 0, A_i \text{ і } A_j \text{ не зв'язані} \end{cases}$; A_{ij} – матриця суміжності, що вказує на наявність або відсутність комунікаційного каналу між агентами.

Після обрання, агент координатор збирає результати оцінок ступеню захищеності інформації з усіх вузлів, об'єднує їх в єдиний звіт і передає ці дані до окремого централізованого вузла, яким керує системний адміністратор, що може переглядати, аналізувати та приймати відповідні рішення на основі отриманих результатів оцінки. Загальний канал комунікаційного зв'язку можна представити як об'єднання спрямованих кроків передачі даних, які разом визначають повну структуру потоку даних під час проведення оцінювання:

$$\phi(t) = \left(\bigcup_{i \neq c(t)} \{A_i \to A_{c(t)}\} \right) \cup \{A_{c(t)} \to C\}, \backslash^*$$

MERGEFORMAT (4)

де $\phi(t)$ – структура потоку даних в момент часу t; $A_{c(t)}$ – агент координатор; A_i – звичайний агент; C – централізований вузол.

Комунікація в системі відбувається у вигляді періодичних повідомлень між агентами. Керуючий агент приймає узагальнені оцінки від підлеглих агентів і формує звіт для центрального вузла. Така ієрархія повідомлень мінімізує обсяг переданої інформації та знижує затримки, що є критичним фактором у великих корпоративних інфраструктурах.

На основі математичної формалізації представленої вище, на рис. 1 зображено високорівневе представлення загальної архітектури запропонованої системи, що функціонує в корпо-

ративній мережі(Corporate Network) і складається із програмних агентів (Agent), які розгортаються на мережевих вузлах (Node), динамічно обраного агента координатора (Coordinator Agent) за результатами проведених виборів, а також централізованого вузла (Centralized Node), який отримує агреговані оцінки стану захищеності даних від керуючого агента.

Внутрішня структура кожного агента показана на рис. 2 і складається з наступних п'яти основних модулів: модуля комунікації (Communication Module), модуля збору даних (Data Collection Module), модуля моніторингу середовища (Environment Module), модуля оцінки інформаційної безпеки (IS Assessment Module) та модуля звітності (Reporting Module).

Модуль зв'язку відповідає за забезпечення обміну даними між агентами та механізму надсилання повідомлень під час усього процесу проведення оцінювання. Це включає обмін оцінками навколишнього середовища під час процесу вибору агента для ролі лідера, передачу результатів оцінки координуючому агенту та синхронізацію операційних завдань за потреби. Модуль збору даних здійснює постійне спостереження за внутрішнім станом та конфігурацією вузла. Він збирає дані, що стосуються безпеки, а також дані про навколишнє середовище з різних підсистем хост машини. Модуль оцінки навколишнього середовища обробляє параметри оточення мережевих вузлів, які були отримані від модуля збору даних. Він може включати такі фактори як використання процесора та оперативної пам'яті, час безперебійної роботи системи, затримку мережі, а також інші параметри стабільності та надійності. Ці показники разом визначають кількісну оцінку навколишнього середовища агентів, що відображає їх операційну стійкість та готовність діяти як координатор. Цей процес може відбуватися періодично або перед кожним циклом оцінки ступеню захищеності даних, дозволяючи системі здійснювати динамічний вибір найбільш підходящого агенту з оптимальними операційними умовами для ролі лідера. Даний механізм вибору програмного компоненту на роль координатора втілює принцип динамічної централізації, що

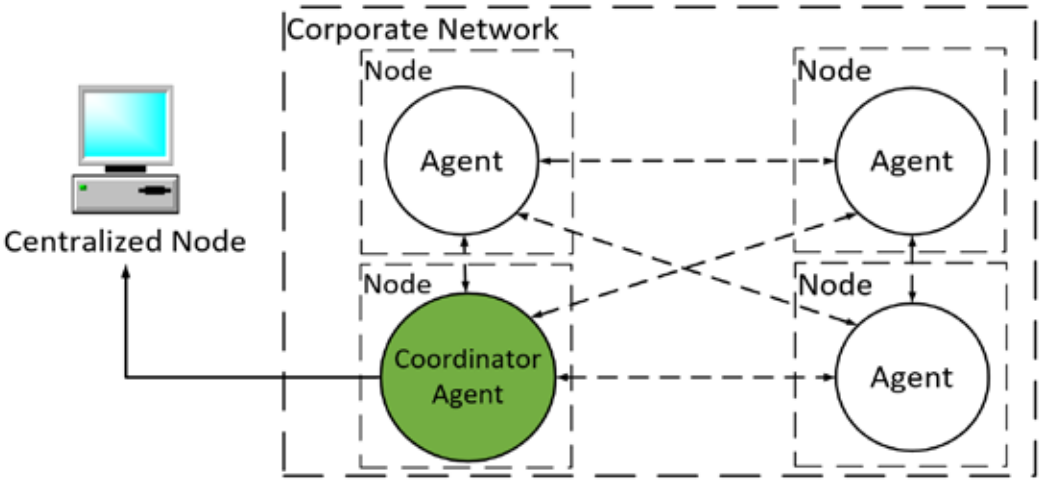

Рис. 1. Високорівневе представлення архітектури системи в корпоративній мережі

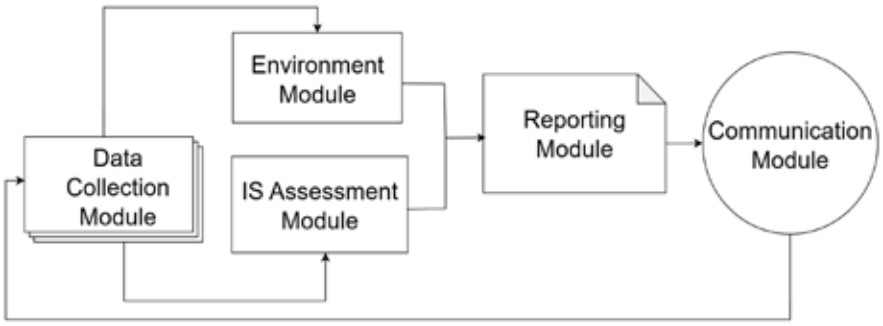

Рис. 2. Внутрішні компоненти програмного агента

забезпечує гнучку адаптацію до постійно змінюваного стану корпоративної мережі.

Модуль оцінювання захищеності інформації відповідає за перетворення необроблених даних індикаторів безпеки, які були отримані від модулю збору інформації, у кількісні показники рівня захищеності. Основу логіки оцінювання становлять індикатори, які базуються на міжнародних стандартах ISO/IEC 27001:2022 [10], ISO/IEC 27002:2022 [13] та NIST SP 800-53 [14]. Ці стандарти визначають правила та технічні заходи безпеки, що відповідають трьом основним принципам інформаційної безпеки, таким як конфіденційність, цілісність та доступність (КЦД). Для кожного індикатора кібербезпеки визначено відповідну математичну модель, яка дозволяє ефективно проводити обчислення кількісних показників на основі конкретних і вимірюваних даних, що отримуються з мережевого вузла. Наприклад, показники можуть включати належну сегментацію прав доступу, наявність та частоту виконання резервних копій даних, дотримання політик паролів або наявність несанкціонованого встановлення програмного забезпечення. Результатом цього процесу є нормалізована кількісна оцінка, яка відображає поточний стан інформаційної безпеки вузла, а також розподіл оцінок за окремим показником. Усі результати оцінювання можуть бути подані у вигляді матриці захищеності, що надає повну картину інформаційної безпеки для кожного вузла мережі:

$$M(t)=\begin{pmatrix} m_{11}(t) & m_{12}(t) & \dots & m_{1k}(t) \\ m_{21}(t) & m_{ij}(t) & \dots & m_{2k}(t) \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1}(t) & m_{n2}(t) & \dots & m_{nk}(t) \end{pmatrix}, \backslash *$$

MERGEFORMAT (5)

де $M(t)$ – матриця безпеки, яка складається з рядків, що відповідають вузлам мережі та стовпців, що відповідають певним показникам безпеки; $m_{ij}(t)$ – кількісний показник оцінки індикатора безпеки j для вузла i; $m_{ij}(t) \in [0,1]$; n – кількість вузлів в мережі; k – загальна кількість вибраних індикаторів безпеки.

Модуль звітності завершує цикл оцінювання, формуючи результати на основі модуля оцінювання захищеності інформації, а також може бути задіяний безпосередньо для процесу проведення вибору агента лідера та включати результати визначення стану навколишнього середовища вузла. Цей модуль формує структуровані звіти, що містять загальну оцінку захищеності інформації або оцінку навколишнього середовища на вузлі. Звіти створюються у стандартизованих форматах, таких як JSON або XML, що забезпечує сумісність із зовнішніми системами та спрощує подальшу агрегацію й перевірку даних. У випадку процесу визначення інформаційної захищеності даних після формування звіти передаються головному агенту за допомогою модуля зв'язку. При проведенні виборів координуючого агенти, результати оцінок навколишнього середовища передаються між агентами через комунікаційні канали з метою визначення нового лідера.

Хоча архітектура системи здебільшого розподілена та агентно-орієнтована, централізований вузол виконує ключову роль точки отримання усієї інформації щодо стану захищеності інформації в корпоративній мережі. Він слугує інтерфейсом між агентами, які розгортаються на вузлах мережі та системними адміністраторами, підтримуючи розширений аналіз, збереження історичних даних, прогнозування та стратегічне планування. Внутрішня структура централізованого вузла складається з чотирьох основних функціональних модулів: модуля представлення, модуля зберігання даних, модуля прогнозування та модуля рекомендацій.

Модуль представлення надає можливість системним адміністраторам переглядати, аналізувати та досліджувати результати оцінювання для усієї корпоративної мережі або окремих її вузлів. Модуль зберігання даних відповідає за безпечне зберігання результатів оцінок інформаційної безпеки, отриманих від агентів через координуючого агента. Кожен запис має позначку визначеного часу проведення процесу оцінювання та пов'язаний з відповідним вузлом, що дозволяє структуровано вести облік для довгострокового відстеження та звітності про відповідність. Цей модуль діє як історичне сховище, яке зберігає інформацію про минулі результати оцінювання станів безпеки та дозволяє зберігання подальших результатів оцінок для їх аналізу. Модуль прогнозування використовує ці структуровані історичні дані для передбачення майбутнього стану інформаційної безпеки в мережі. Використовуючи методи на основі штучного інтелекту та машинного навчання застосовані до часових рядів отриманих показників захищеності даних, цей модуль визначає часові тенденції поступового погіршення певних слабких місць у інформаційній безпеці. Його результати включають прогнози майбутніх станів безпеки як на рівні окремих вузлів, так і для корпоративної мережі в цілому. Це дозволяє адміністраторам зрозуміти, чи може сис-

тема стати більш вразливою з часом і визначити пріоритети превентивних дій. Модуль рекомендацій розширює функціональність прогнозування, перетворюючи прогнозовані результати захищеності на цілеспрямовані практичні рекомендації. На основі результатів, отриманих модулем прогнозування, а також наявних даних минулих оцінювань, цей компонент формулює рекомендації, спрямовані на боротьбу із потенційними інцидентами безпеки даних та зміцнення загальної стійкості мережі.

Інтеграція модулів прогнозування та рекомендацій робить можливим перехід від реактивного до проактивного управління безпекою, що є важливим кроком до побудови самокерованих систем моніторингу інформаційної безпеки нового покоління.

Загалом функціонування системи передбачає циклічне виконання етапів збору, обробки та аналізу інформації. У кожному циклі агенти проводять локальне оцінювання, передають результати головному агенту, який агрегує дані та надсилає їх на централізований вузол. Координатор обирається динамічно на основі оцінки поточного технічного стану вузлів, що забезпечує збалансованість навантаження і відмовостійкість системи. Якщо керуючий програмний агент виходить із ладу, тоді ініціюється процедура його переобрання без порушення загального процесу оцінювання. Передбачено два режими роботи системи, а саме періодичний, який виконується через задані часові інтервали і запитуваний, що активується вручну адміністратором. Така організація дозволяє адаптувати систему до різних сценаріїв роботи корпоративної мережі.

Розроблена система забезпечує комплексне оцінювання стану інформаційної безпеки корпоративної мережі в умовах динамічної зміни її структури. Використання агентно-орієнтованого підходу дозволило поєднати розподілене оцінювання безпеки з централізованою аналітикою, забезпечивши автономність, масштабованість і надійність.

Дослідження ефективності. Для оцінювання ефективності запропонованої агентно-орієнтованої архітектури було проведено експериментальне дослідження, метою якого стало визначення здатності системи підтримувати стабільність, доступність і відмовостійкість у динамічних умовах корпоративного середовища. Особливу увагу приділено оцінці архітектурних характеристик, які відображають роботу системи під час змін у складі або стані вузлів.

Експеримент проводився у віртуалізованому середовищі, що імітувало корпоративну мережу з 50 вузлів. На кожному вузлі було розгорнуто програмного агента, який здійснював локальну оцінку стану інформаційної безпеки, обмін повідомленнями з іншими агентами та взаємодію з координатором у межах циклів оцінювання. Один із агентів динамічно обирався у ролі лідера, який відповідав за збір, агрегування та передачу результатів оцінки до централізованого вузла. Для моделювання роботи системи використовувались синтетичні дані, що дозволяло варіювати умови мережевого навантаження, кількість активних вузлів і часові затримки у каналах зв'язку.

Було змодельовано чотири сценарії, що відображають типові умови функціонування корпоративної мережі.

Перший сценарій представляє номінальний режим роботи при якому система працює стабільно без збоїв або перевантажень і при цьому усі вузли доступні.

У другому сценарії відбувається втрата координатора, тобто один із вузлів, що виконував роль керуючого агента стає недоступним і тому система вимушена автоматично ініціювати процес переобрання нового лідера.

При третьому сценарії вводиться штучне перевантаження вузлів у якому 25% вузлів працюють із підвищеним навантаженням, що впливає на час обробки повідомлень та комунікаційні затримки.

Останній, четвертий сценарій вводить часткові збої у комунікації при яких у 10% вузлів періодично виникають короткочасні відключення зв'язку та втрата повідомлень, що перевіряє здатність системи до відновлення координації.

Для кожного сценарію проводилося кількісне вимірювання таких показників як: коефіцієнт доступності у відсотках, що показує частку часу протягом якого система залишалася працездатною; часова затримка переобрання координатора у секундах, що відображає середній час, який необхідний для повторного вибору керуючого агента після виявлення відмови; показник комунікаційних витрат, який показує відсоток мережевого трафіку, що припадає на службові координаційні повідомлення між агентами по відношенню до загального циркулюючого мережевого трафіку; коефіцієнт відмовостійкості у відсотках, що показує відсоток успішних циклів оцінювання після збоїв.

Отримані результати свідчать про високу стабільність і адаптивність архітектури у різних експлуатаційних умовах. Коефіцієнт доступності системи залишався в межах від 95 до 100%, що

Таблиця 1

Результати експериментального дослідження функціонування системи при різних сценаріях

Показник	Сценарій 1	Сценарій 2	Сценарій 3	Сценарій 4
Коефіцієнт доступності, %	100	98,7	99,1	95,2
Часова затримка переобрання координатора, с	–	2,6	1,9	3,4
Комунікаційні витрати, %	5,0	5,8	6,2	6,8
Коефіцієнт відмовостійкості, %	100	97,3	98,5	94,5

демонструє здатність підтримувати безперервну роботу навіть за часткових відмов. Найбільше зниження спостерігалось у четвертому сценарії, що зумовлено тривалими втратами зв'язку між вузлами. Часова затримка переобрання агента лідера коливалася в межах від 1,9 до 3,4 с, що є прийнятним для систем із розподіленою логікою управління. Це підтверджує ефективність реалізованої схеми динамічної централізації за якої новий координатор визначається оперативно без порушення процесів оцінювання. Комунікаційні витрати для міжагентної взаємодії не перевищили 7% від загального обсягу трафіку навіть у найскладніших умовах, що свідчить про оптимальну організацію процесу спілкування між агентами. Коефіцієнт відмовостійкості перевищував 94%, тобто більшість циклів оцінювання завершувалися успішно навіть після короткочасних збоїв або втрат головного керуючого агенту.

Проведений експеримент підтвердив здатність розробленої агентно-орієнтованої архітектури забезпечувати високий рівень доступності, відмовостійкості та ефективної самоорганізації навіть за умов динамічних змін мережевого середовища. Система підтримує стабільний обмін між агентами та мінімальний рівень комунікаційних витрат відведених для частки службового трафіку, що свідчить про її придатність для подальшої інтеграції у корпоративні інфраструктури. Отримані результати створюють основу для подальших досліджень, спрямованих на вдосконалення методів організації функціонування та оптимізації міжагентної координації.

Висновки. Отже, було представлено концептуальну архітектуру агентно-орієнтованої розподіленої системи з елементами динамічної централізації, яка призначена для оцінювання стану захищеності даних в корпоративних мережах. Запропонована архітектура базується на сукупності автономних агентів, які розгортаються на окремих вузлах мережі та здійснюють збір даних, обчислення локальних показників захищеності та взаємодію між собою для вибору агента лідера. Такий агент координатор виконує роль динамічного центру керування, агрегує результати оцінювання та передає їх до централізованого вузла в якому можливе подальше прогнозування змін стану безпеки за допомогою модулів аналітики, доступ до яких мають системні адміністратори.

Практична цінність запропонованої архітектури полягає у створенні універсального підґрунтя для побудови інтелектуальних систем оцінювання стану захищеності даних корпоративних мереж. Її структура забезпечує кількісне вимірювання рівня захищеності даних на основі формалізованих показників, що базуються на основі міжнародних стандартів кібербезпеки, а саме ISO/IEC 27001:2022, ISO/IEC 27002:2022 та NIST SP 800-53. Завдяки модульності та агентно-орієнтованому підходу, архітектура може бути адаптована до різних типів корпоративних інфраструктур, забезпечуючи масштабованість, гнучкість та розподілення обчислювального навантаження між вузлами. Важливою особливістю системи є механізм динамічної централізації, який дозволяє автоматично переобирати координатора та підтримувати стабільність функціонування навіть за умов часткових відмов або змін у мережі. Крім того, на централізованому вузлі присутній функціонал прогнозування станів інформаційної безпеки, що базується на аналізі часових рядів попередніх оцінок та використовує елементи машинного навчання і штучного інтелекту. Це надає можливість не лише оцінювати поточний рівень захищеності, а й передбачати його майбутні зміни, своєчасно виявляючи тенденції деградації безпеки. Таким чином, система формує інформаційно-аналітичну основу для стратегічного планування, підвищення рівня кіберстійкості та оптимізації заходів із захисту корпоративних ресурсів.

Подальші дослідження будуть сконцентровані на впровадження розробленої системи у реальні корпоративні мережі великих підприємств для перевірки її працездатності та ефективності в реальних умовах експлуатації. Особлива увага приділятиметься подальшому розвитку механізмів динамічної централізації з метою оптимізації процесу координації агентів і зниження часових затримок при переобранні лідера. Також буде розглянута можливість інтеграції системи із зовнішніми інформаційними ресурсами та платформами корпоративної безпеки для створення більш комплексного середовища оцінювання.

Список літератури:

1. Jain L., Bhushan B. Systematic Analysis of Common Cyber Attacks and Their Mitigation Techniques. *International Conference on Emerging Technologies and Innovation for Sustainability (EmergIN)*. Greater Noida, India. 2024. P. 519–524. DOI: 10.1109/EmergIN63207.2024.10961137.

2. Pandya J. J., Kharote P. Review on cybersecurity and techniques. *In International Conference on Smart Computing and Communication*. Springer, Singapore. 2024. Vol. 946. P. 285–300. DOI: 10.1007/978-981-97-1323-3_24

3. Kodituwakku A., Gregor J. Indepth: A distributed data collection system for modern computer networks. *Electronics*. 2025. Vol. 14, No. 10. P. 1974. DOI: 10.3390/electronics14101974.

4. Savenko B., Kashtalian A., Lysenko S., Savenko O. Malware Detection By Distributed Systems with Partial Centralization. *In 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*. Dortmund, Germany. 2023. Vol. 1. P. 265–270. DOI: 10.1109/IDAACS58523.2023.10348773.

5. SentinelOne Singularity. URL: https://www.sentinelone.com/platform/endpoint-security/(дата звернення. 25.10. 2025).

6. Chen Y., Layeghy S., Manocchio L.D., Portmann M. P4-NIDS: High-Performance Network Monitoring and Intrusion Detection in P4. *In Intelligent Computing-Proceedings of the Computing Conference*. Springer, Cham. 2025. Vol. 1426. P. 355–373. DOI: 10.1007/978-3-031-92611-2_24.

7. Genuario F., Santoro G., Giliberti M., Bello S., Zazzera E., Impedovo D. Machine Learning-Based Methodologies for Cyber-Attacks and Network Traffic Monitoring: A Review and Insights. *Information*. 2024. Vol. 15, No. 11. P. 741. DOI: 10.3390/info15110741

8. Bedratyuk L. Savenko O. The star sequence and the general first Zagreb index. *MATCH Commun*. Math. Comput. Chem. 2018. Vol. 79. P. 407–414.

9. Tonge A. S., Baniya B. K., GC D. Efficient, scalable, and secure network monitoring platform: Self-contained solution for future smes. *Network*. 2025. Vol. 5, No. 3. P. 36. DOI: 10.3390/network5030036.

10. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: International Organization for Standardization, 2022. 35 p.

11. ESET PROTECT Enterprise. URL: https://www.eset.com/me/business/enterprise-protection(дата звернення. 25.10. 2025).

12. Yuan Q., Meng Q., Tao J., Li G., Fei J., Lu B., Wang Y. Multi-Agent for Network Security Monitoring and Warning: A Generative AI Solution. *In IEEE Network*. 2025. Vol. 39, No. 5. P. 114–121. DOI: 10.1109/MNET.2025.3579001.

13. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. Geneva: International Organization for Standardization, 2022. 69 p.

14. Force J. T. Security and Privacy Controls for Federal Information Systems and Organizations. *NIST Special Publication 800-53*. 2020. Rev. 4. DOI: 10.6028/NIST.SP.800-53r4.

15. Lysenko S., Savenko B. Distributed Discrete Malware Detection Systems Based on Partial Centralization and Self-Organization. International Journal of Computing. 2023. Vol. 22. P. 117–139. DOI: 10.47839/ijc.22.2.3082.

16. Sheeraz M., Paracha M. A., Haque M. U., Durad M. H., Mohsin S. M., Band S. S., Mosavi A. Effective security monitoring using efficient SIEM architecture. *Hum.-Centric Comput. Inf. Sci*. 2023. Vol. 13. P. 1–18. DOI: 10.22967/HCIS.2023.13.023.

17. CrowdStrike Falcon. URL: https://www.crowdstrike.com/en-us/platform (дата звернення. 25.11. 2025).

18. Şenol M. Innovation in Corporate Cyber Security. In *2023 4th International Informatics and Software Engineering Conference (IISEC)*. Ankara, Turkiye, 2023. P. 1–6. DOI: 10.1109/IISEC59749.2023.10390993.

19. Noviyarto H., Samopa F., Setiawan B. Security Audit Process Design Based on SIEM and CSPM Integration with Design Science Research Methodology Approach. In *2025 International Conference on Data Science and Its Applications (ICoDSA)*. Jakarta, Indonesia, 2025. P. 679–685. DOI: 10.1109/ICoDSA67155.2025.11157488.

20. Symantec Endpoint Security Complete. URL: https://www.broadcom.com/products/cybersecurity/endpoint/end-user/complete (дата звернення. 25.11. 2025).

21. Splunk Enterprise Security. URL: https://www.splunk.com/en_us/products/enterprise-security.html (дата звернення. 25.11. 2025).

22. Perone S., Faramondi L., Guarino S., Nobili M., Setola R., Del Prete E., Laurenda A. ZADIG: A novel Extended Detection and Response System. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*. London, United Kingdom, 2024. P. 688-693. DOI: 10.1109/CSR61664.2024.10679420.

23. Fredrick S., Singh P. Cyber Threat Monitoring and Incident Response with IntelliWatch SIEM. In *2023 International Conference on Sustainable Communication Networks and Application (ICSCNA)*. Theni, India. IEEE, 2023. P. 209–215. DOI: 10.1109/ICSCNA58489.2023.10370155.

24. Qin J., Yu D., Wang H. Research on distribution network monitoring and fault location based on edge computing. *In International Conference on Frontier Computing*. Singapore: Springer Nature Singapore. 2023. P. 260–265. DOI: 10.1007/978-981-99-9538-7_39.

25. Ayu M. A., Erlangga D., Mantoro T., Handayani D. Enhancing Security Information and Event Management (SIEM) by Incorporating Machine Learning for Cyber Attack Detection. In *2023 IEEE 9th International Conference on Computing, Engineering and Design (ICCED)*. Kuala Lumpur, Malaysia. 2023. P. 1–6. DOI: 10.1109/ICCED60214.2023.10425288.

Oliinyk P.A., Savenko O.S., Hnatyuk O.I. CONCEPTUAL SYSTEM'S ARCHITECTURE FOR ASSESSING INFORMATION SECURITY IN CORPORATE NETWORKS

The article highlights the urgent problem of assessing the state of information security of corporate systems in the context of the increasing resilience of distributed corporate networks and high requirements for their reliability and stability. An analysis of modern scientific research and commercial solutions in the field of monitoring, management and analytics of cybersecurity was conducted, as a result of which a number of limitations were identified. In addition, the latest existing approaches, focused on incident detection or event monitoring, do not reflect a comprehensive quantitative assessment of the level of security of information resources based on standardized indicators. Also, such systems lack mechanisms built on the basis of artificial intelligence and machine learning, which would allow making predictive assessments and modeling the dynamics of changes in the security state over time. In addition, modern systems lack focus on developed mechanisms for flexible coordination of interaction between elements of the distributed environment, which can lead to excessive load on central nodes, reduce the efficiency of data exchange and lose stability in the event of failures or changes in the network topology.

In order to eliminate the identified shortcomings, a conceptual architecture of an agent-oriented distributed system with elements of dynamic centralization is proposed, which provides automated assessment of the state of information security in corporate environments, which does not require the involvement of system administrators. In the proposed system, software agents are installed on the nodes of the corporate network and consider the assessment of the current level of data security based on formalized indicators consistent with international cybersecurity standards. The interaction between agents is organized according to the principle of dynamic centralization, which allows adaptively changing the role of the coordinator, ensuring high fault tolerance and balanced load in the system. The centralized node in the architectural system performs the functions of an analytical and predictive center, which allows not only to summarize the results of the assessment, but also to predict trends in changes in the level of security over time. An experiment was conducted to determine the efficiency of the system in various operating scenarios aimed at testing the stability, reliability and efficiency of its architecture. The evaluation is carried out using a number of system metrics that reflect the level of availability, fault tolerance, coordination delay, and communication costs. The results of the experiment confirmed the feasibility of using an agent-oriented approach for building distributed information security assessment systems.

Key words: *agent-oriented system, corporate network, distributed systems, dynamic centralization, software agent, information security assessment, NIST SP 800-53, ISO/IEC 27001:2022, ISO/IEC 27002:2022.*

Дата надходження статті: 12.11.2025
Дата прийняття статті: 02.12.2025
Опубліковано: 30.12.2025