DOI: https://doi.org/10.25140/2411-5363-2025-3(41)-158-168
УДК 004.056:004.8

Алла Григорівна Гребенник[1], Олексій Ігорович Трунов[2]

[1]старший викладач кафедри кібербезпеки та математичного моделювання
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: grebennik.alla@gmail.com. **ORCID:** https://orcid.org/0000–0002–7464–1412
Scopus Author ID: 57219054928

[2]аспірант, викладач кафедри інформаційних технологій та програмної інженерії
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: alexeytrunov1995@gmail.com. **ORCID:** https://orcid.org/0009-0002-0321-2669
Scopus Author ID: 59337119500

АЛГОРИТМ ВИЗНАЧЕННЯ АГРЕГОВАНОЇ ДИНАМІЧНОЇ ОЦІНКИ СТАНУ БЕЗПЕКИ МЕРЕЖЕВОГО КОНТЕНТУ

Зростання складності кіберзагроз та обсягів мережевого контенту висуває проблему недостатності існуючих підходів до оцінки стану інформаційної безпеки. Актуальним завданням є агрегація різнорідних, неповних та неточних даних, що надходять від численних систем захисту (SIEM, IDS/IPS, антивіруси, ШІ-системи) у єдиний інтегральний показник, що дозволяє ухвалювати обґрунтовані рішення в умовах невизначеності.

У результаті дослідження запропоновано алгоритм визначення агрегованої динамічної оцінки стану безпеки мережевого контенту. Алгоритм інтегрує два компоненти: нечітку базову оцінку, що враховує статичні архітектурні характеристики системи на основі апарату нечіткої логіки, та динамічну оцінку, що кількісно відображає рівень поточної загрози на основі даних від інтелектуальних систем аналізу. Запропонований підхід дозволяє отримати єдиний інтегральний показник стану безпеки в режимі, наближеному до реального часу, та використовувати його як тригер для реалізації механізмів адаптивного управління та автоматизованого реагування на інциденти.

Ключові слова: *інформаційна безпека; мережевий контент; агрегована оцінка; динамічна оцінка; штучний інтелект; нечітка логіка; адаптивне управління.*

Рис.: 1. Табл.: 1. Бібл.: 16.

Актуальність теми дослідження. Метою застосування засобів захисту корпоративної мережі є ефективна та оперативна протидія всім потенційно можливим інформаційним загрозам. У цьому контексті аналіз мережевого контенту відіграє критично важливу роль, оскільки він є одночасно як вектором для поширення атак, так і ключовим джерелом інформації для систем моніторингу та реагування. Однак сучасні корпоративні мережі функціонують в умовах невпинного зростання обсягів даних та перманентної еволюції загроз. Це змушує приймати рішення щодо класифікації контенту та вибору механізмів реагування в умовах значної невизначеності, яка породжується неповнотою, неточністю та різнорідністю даних.

Зазначені обставини об’єктивно вимагають розробки нового науково-методичного апарату, основу якого повинні складати інтелектуальні алгоритми, здатні виконувати комплексну оцінку захищеності та прогнозування загроз на основі безперервного аналізу контенту.

Постановка проблеми. Сучасні корпоративні мережі функціонують в умовах експоненційного зростання обсягів мережевого контенту та перманентної еволюції загроз. Це обумовлює критичну необхідність у розробці проактивних механізмів захисту. Актуальність дослідження зумовлена низкою нерозв’язаних науково-практичних проблем, центральною з яких є відсутність єдиної методології для комплексної оцінки стану безпеки мережевого контенту в умовах невизначеності.

Ключові проблеми, що потребують вирішення, полягають у наступному:

1. Проблема агрегації різнорідних даних. Засоби захисту (SIEM, IDS/IPS, антивіруси, ШІ-системи) генерують величезну кількість різнорідних за своєю природою показників: від статичних характеристик конфігурації системи до динамічних вердиктів про виявлені аномалії. Відсутній формалізований підхід, який би дозволяв агрегувати ці неповні, неточні та різнорідні дані в єдиний, інтегрований показник безпеки.

2. Проблема динамічної оцінки. Адаптивний характер сучасних кібератак, які використовують багатовекторні стратегії та приховані канали передачі даних, робить статичні або періодичні оцінки неефективними. Є гостра потреба в механізмі динамічної оцінки, здатному оновлювати стан безпеки в режимі, наближеному до реального часу, реагуючи на постійний потік змін мережевого контенту.

3. Проблема формалізації критеріїв. Складність формалізації критеріїв оцінки рівня безпеки, які мають комплексно враховувати як статичні (архітектурні) аспекти, так і динамічні (подієві) характеристики, вимагає застосування інтелектуальних підходів, здатних працювати з нечіткими та неповними вхідними даними.

Зазначені обставини об'єктивно вимагають розробки нового науково-методичного апарату. Таким чином, актуальною науковою задачею є розробка алгоритму визначення агрегованої динамічної оцінки стану безпеки мережевого контенту, який би забезпечував синтез даних із різнорідних джерел та надавав обґрунтовану основу для ухвалення рішень щодо механізмів реагування, гарантуючи адекватну протидію як відомим, так і раніше невизначеним кіберзагрозам.

Аналіз останніх досліджень і публікацій. Основоположні принципи захисту та моніторингу [1] створюють загальну рамку для побудови систем безпеки. Існуючі методики агрегації метрик [2; 3] та апарат нечіткої логіки для обробки невизначених даних [4] надають теоретичну основу для інтеграції показників. З розвитком загроз ключовою стала концепція адаптивної безпеки [5], рушійною силою якої є методи машинного навчання (МН) [6], що дозволяють виявляти аномалії безпосередньо в трафіку на основі якісних наборів даних [7]. Найсучасніші дослідження пропонують високоточні системи на основі штучного інтелекту (ШІ) для виявлення складних цільових атак (APT) [8] та превентивного виявлення загроз за допомогою генеративно-змагальних мереж (GAN) [9].

Виділення недосліджених частин загальної проблеми. Незважаючи на значний прогрес, залишається невирішеною проблема цілісної оцінки стану безпеки мережевого контенту. Сучасні засоби захисту генерують величезну кількість різнорідних показників (статичні конфігурації, динамічні вердикти ШІ-систем), однак відсутній формалізований підхід для їх агрегації у єдиний, інтерпретований індикатор. Крім того, адаптивний характер кібератак вимагає механізму динамічної оцінки, здатному оновлювати стан безпеки в режимі реального часу.

Метою статті є розробка алгоритму визначення агрегованої динамічної оцінки стану безпеки мережевого контенту. Цей алгоритм має виступати як інтеграційна платформа (*fusion engine*), що вирішує зазначені проблеми, об'єднуючи різнорідні показники безпеки в єдиний індикатор для запуску механізмів адаптивного реагування.

Виклад основного матеріалу. У межах дослідження запропонована модифікація алгоритму аналізу захищеності мережевого контенту на базі вже існуючих підходів [10] із залученням апарату нечіткої логіки та штучного інтелекту [11; 12]. Застосування методів технології «м'яких обчислень» для модифікації дозволяє алгоритмам набути властивостей, що є перспективними щодо захисту інформації: адаптивність, навчання, розпізнавання тощо [13]. Їх застосування закономірно щодо вимог до інформаційно-комунікаційних систем, які протягом життєвого циклу постійно змінюють свої стани, а рівень їх захищеності повинен бути максимально стабільним і таким, що відповідає заданим вимогам. Тільки такі системи мають високу ймовірність протистояти новим, раніше невідомим загрозам.

Для проведення аудиту мережевого контенту щодо забезпечення інформаційної безпеки розглянемо критерії і метрики рівня захищеності. Серед них:

1. Функціональні критерії оцінки рівня захищеності, що оцінюють конкретні функції безпеки, які надаються системою, безпосередньо або опосередковано через мережевий контент.

2. Критерії гарантії безпеки, що оцінюють рівень довіри до того, що функції безпеки реалізовані коректно та ефективно, які можуть включати перевірку через мережевий контент.

3. Додаткові метрики аудиту, пов'язані з контент-аналізом, що характеризують взаємодію користувачів з контентом, які є основою для його подальшого аналізу в контексті ІБ, або є результатами такого аналізу.

Важливо зазначити, що критерії і метрики можуть мати як якісні, так і кількісні аспекти залежно від того, як вони вимірюються та інтерпретуються в конкретному аудиті (табл. 1).

Таблиця 1 – Критерії для аналізу мережевого контенту щодо забезпечення інформаційної безпеки

Категорія критерію	Фактор / Сімейство вимог ISO/IEC 15408 [14]	Тип (якісний / кількісний / змішаний)	Опис / Призначення (аналіз мережевого контенту в контексті ІБ)
1. Функціональні критерії оцінки рівня захищеності			
1	2	3	4
Аудит безпеки	FAU: security audit	Змішаний	Якість журналювання подій безпеки. Важливо для аналізу мережевих подій.
Зв'язок	FCO: communication	Якісний	Безпека комунікацій (шифрування, цілісність). Аналізується через мережевий контент.
Криптографічна підтримка	FCS: cryptographic support	Змішаний	Використання криптографічних засобів. Аналіз контенту для ідентифікації шифрування.
Захист даних користувача	FDP: user data protection	Змішаний	Механізми захисту даних. Аналіз контенту на предмет витоків конфіденційної інформації.
Ідентифікація та аутентифікація	FIA: identification and authentication	Змішаний	Процеси ідентифікації/аутентифікації. Аналіз трафіку для виявлення атак.
Секретність	FPR: privacy	Якісний	Заходи щодо конфіденційності. Аналіз контенту для виявлення порушень.
Використання ресурсів	FRU: resource utilisation	Змішаний	Управління ресурсами для запобігання відмові в обслуговуванні. Аналіз контенту для виявлення DoS/DDoS.
Доступ до ЦОО (цільового об'єкта оцінки)	FTA: TOE access	Якісний	Механізми доступу до системи. Аналіз контенту для моніторингу несанкціонованих спроб доступу.
Надійний маршрут/канал	FTP: trusted path/ channels	Якісний	Наявність захищених каналів зв'язку. Аналіз контенту для верифікації їх безпеки.
2. Критерії гарантії безпеки (Assurance Requirements)			
Життєвий цикл та розробка	ADT: Development; ALC: Life-cycle Support	Якісна	Безпека процесів розробки, тестування, підтримки ПЗ/обладнання. Впливає на безпеку контенту.
Тестування	ATE: Tests	Змішаний	Адекватність тестування функцій безпеки. Частиною аналізу мережевого контенту є оцінювання результатів тестів на проникнення.
Оцінка вразливих місць	AVA: Vulnerability assessment	Змішаний	Виявлення, аналіз, оцінка вразливостей мережевого контенту.
Конфігураційне управління	ACM: Configuration Management	Якісна	Контроль за змінами та конфігурацією. Знижує ризик вразливостей через контент.

Закінчення табл. 1

1	2	3	4
Доставка та експлуатація	ADO: Delivery and Operation	Якісна	Безпечні процедури доставки/встановлення. Забезпечує безпечну доставку контенту (оновлень).
Керівництво (документація)	AGD: Guidance Documents	Якісна	Якість документації з безпечної експлуатації. Включає інструкції щодо роботи з мережевим контентом.
3. Додаткові метрики аудиту, пов'язані з контент-аналізом			
Кількість інцидентів безпеки	Метрика ефективності (SIEM, SOAR)	Кількісна	Зареєстровані інциденти безпеки. Виявляються та відстежуються через аналіз мережевого контенту.
Час виявлення та реагування	Метрика продуктивності (SOAR)	Кількісна	Час від інциденту до його усунення. Ефективний аналіз контенту скорочує цей час.
Відсоток відповідності вимогам	Метрика відповідності (Compliance)	Кількісна	Дотримання політик ІБ та стандартів. Перевіряється аналізом контенту, якщо вимоги стосуються мережевої активності.
Результати тестування на проникнення та сканування вразливостей	Метрика тестування (Pentest)	Змішана	Виявлені вразливості, успішність проникнення. Базується на аналізі мережевого трафіку тестів.
Тональність згадок (Sentiment Analysis)	Дані з відкритих джерел (OSINT)	Якісна	Емоційне забарвлення згадок про систему. Моніторинг репутації та загроз.
Авторитет джерела (Source Authority)	Дані аналізу контенту	Якісна	Оцінка надійності джерела мережевого контенту. Критично для виявлення фішингу, дезінформації.
Репутація IP-адрес/доменів	Дані Threat Intelligence	Якісна	Оцінка відомої загрози IP-адрес/доменів. Інтеграція з базами репутацій.
Виявлення шкідливого коду/файлів	Метрика захисту (Antivirus, EDR, Sandbox)	Кількісний	Ідентифікація/блокування шкідливого ПЗ у мережевому контенті.
Виявлення спроб фішингу/шахрайства	Метрика захисту (Email Gateway, NLP)	Якісна	Ідентифікація ознак фішингових атак у контенті.

Джерело: розроблено авторами.

У розробці були використані лише функціональні критерії оцінки рівня захищеності та додаткові метрики аудиту, оскільки вони повною мірою описують ефективність виявлення, класифікації та реагування на потенційно шкідливий або невідповідний мережевий контент, забезпечуючи адекватну оцінку здатності системи до запобігання, моніторингу та протидії кіберзагрозам в умовах динамічного мережевого середовища.

Щодо критеріїв гарантії безпеки, то вони є методологічними та валідаційними факторами, що забезпечують достовірність і якість оцінки «факторів впливу», зокрема:

– аналіз вразливостей (AVA) інформує про довіру до оцінок статичних (функціональних) факторів та допомагає зрозуміти потенційну небезпеку динамічних подій;

– тестування гарантії (ATE) підтверджує належне функціонування статичних критеріїв;

– конфігураційне управління (ACM) підтримує визначений рівень якості статичних критеріїв;

– управління життєвим циклом та розробкою (ALC) впливає на загальну якість функціоналу.

Таким чином, критерії гарантії безпеки є не динамічними вхідними даними, а мета-критеріями, що формують якість та достовірність початкових даних та процедур оцінки, що є частиною валідації та забезпечення якості алгоритму.

Для забезпечення комплексного та адаптивного захисту інформаційних ресурсів пропонується алгоритм визначення агрегованої динамічної оцінки стану безпеки мережевого контенту (рис. 1).

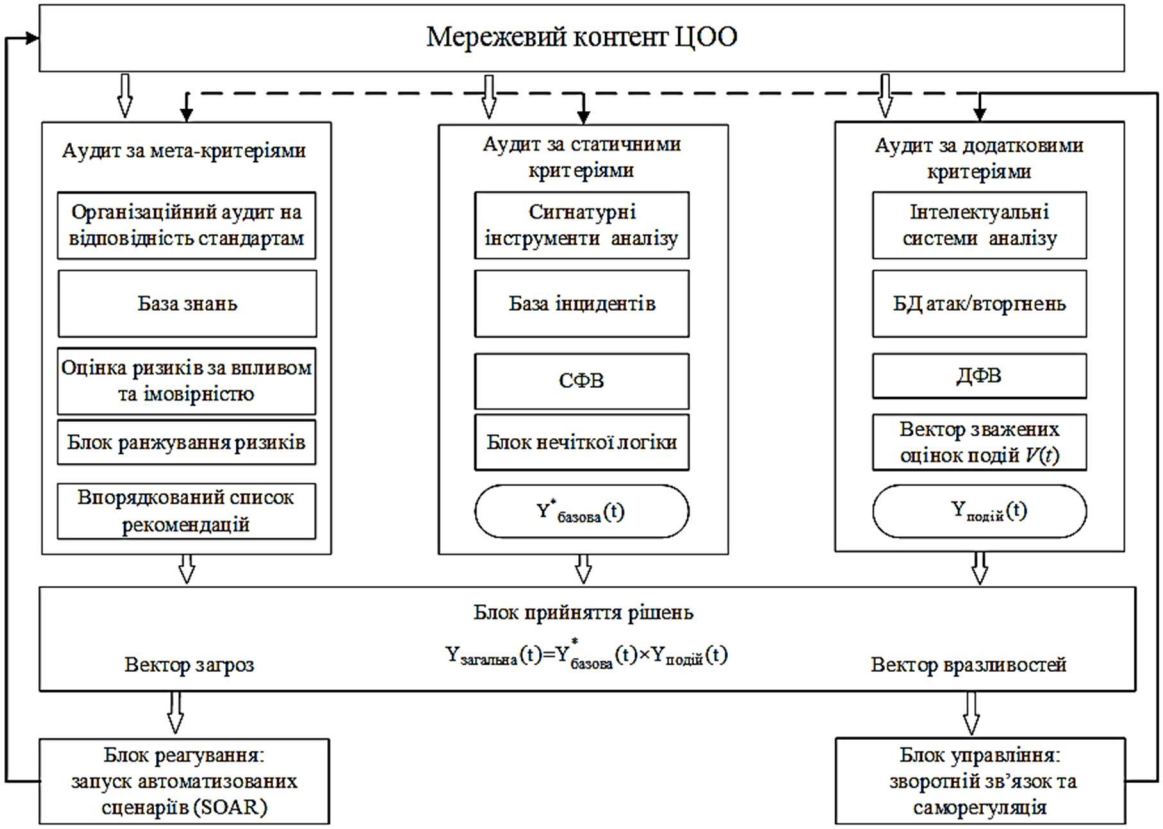

Рис. 1. Алгоритм визначення агрегованої динамічної оцінки стану безпеки мережевого контенту

Джерело: розроблено авторами.

Цей алгоритм дозволяє в режимі, наближеному до реального часу, інтегрувати як статичні, так і динамічні фактори, що впливають на рівень інформаційної безпеки.

В основі методології лежить застосування апарату нечіткої логіки для формалізації та обробки якісних експертних оцінок статичних параметрів системи захисту, а також їх подальша комбінація з кількісними показниками подій безпеки, що моніторяться. Підсумкова інтегральна оцінка (Y) служить індикатором поточного рівня захищеності та є тригером для активації механізмів адаптивного управління безпекою [15].

Розроблений алгоритм передбачає три ключові етапи: визначення нечіткої базової оцінки; визначення оцінки впливу подій; визначення загальної інтегральної оцінки.

Етап 1. *Визначення нечіткої базової оцінки* ($\tilde{Y}_{\text{базова}}$). Базова оцінка відображає фундаментальний рівень захищеності системи, що базується на її відносно стабільних характеристиках – статичних факторах впливу (СФВ). Їх визначення відбувається на етапі початкової підготовки та конфігурації.

1.1. Вибір та формалізація СФВ. Статичні фактори впливу є фундаментальними, відносно незмінними характеристиками системи захисту, що відображають її архітектурну

надійність та відповідність стандартам. Вибір СФВ базується на функціональних критеріях безпеки міжнародного стандарту ISO/IEC 15408 (FAU, FCO, FCS, FDP, FIA, FPR, FRU, FTA, FTP), що наведені в табл. 1. Кожен обраний критерій розглядається як лінгвістична змінна $\tilde{x}_i$, для якої визначаються терм-множини (на кшталт, {незадовільний, достатній, оптимальний}) та будуються відповідні функції належності $\mu(x)$.

1.2. Модель розрахунку. Для обчислення базової оцінки використовується нечітка регресійна модель. Загальний вигляд моделі для розрахунку нечіткої базової оцінки стану безпеки є таким:

$$\tilde{Y}_{\text{базова}} = \tilde{\beta}_0 \oplus \sum_{i=1}^{n} \tilde{\beta}_i \otimes \tilde{x}_i \ \oplus \sum_{u,j=1}^{n} \tilde{\beta}_{ju} \otimes \tilde{x}_j \otimes \tilde{x}_u \ \ (j \neq u), \quad (1)$$

де $\tilde{Y}_{\text{базова}}$ – нечітка базова оцінка функціональної безпеки мережевого контенту;

n – загальна кількість статичних факторів моделі;

$\tilde{x}_i$ – лінгвістична змінна, що відповідає *і-му* статичному фактору;

$\tilde{\beta}_0, \tilde{\beta}_i, \tilde{\beta}_{ju}$ – нечіткі коефіцієнти, що визначають вагу компонентів моделі [16]. Зокрема: $\tilde{\beta}_0$ – нечіткий вільний член (базове зміщення), $\tilde{\beta}_i$ – нечітка вага, що визначає важливість *i*-го статичного фактору, $\tilde{\beta}_{ju}$ – нечітка вага, що визначає силу та характер взаємодії між *j*-м та *u*-м факторами;

$\oplus, \otimes$ – операції нечіткого додавання та нечіткого множення відповідно.

Таким чином, така модель коректно обробляє та поширює невизначеність на кожному етапі розрахунку – від вхідних лінгвістичних оцінок до параметрів самої моделі, що дозволяє отримати більш адекватний та обґрунтований кінцевий результат.

На етапі динамічної оцінки розрахунок здійснюється за допомогою моделі (1) з використанням поточних значень $\tilde{x}_i(t)$. Отримане нечітке значення $\tilde{Y}_{\text{базова}}(t)$ за допомогою методу дефаззифікації перетворюється в чітке числове значення $Y^*_{\text{базова}}(t)$ у діапазоні [0, 1].

Eman 2. На цьому кроці визначаються джерела динамічних даних. На відміну від простих лічильників, ДФВ є інтерпретованими висновками інтелектуальних систем аналізу, згаданих у працях [6], [8], [9]. Кожен такий висновок розглядається як окремий динамічний фактор (S_k). Прикладами таких факторів є:

– імовірність фішингової атаки (S_1) – чисельне значення від 0 до 1, згенероване моделлю обробки природної мови (NLP), яка аналізує текстовий контент та метадані мережевих сесій;

– рівень аномальності трафіку (S_2) – оцінка від 0 до 1, видана моделлю глибокого навчання (наприклад, Autoencoder), що навчена на нормальній поведінці мережі;

– оцінка загрози APT (S_3) – вердикт системи на основі ШІ (згідно з підходом [8]), що аналізує ланцюжки подій у часі;

– детектування атаки GAN-системою (S_4) – бінарний (0 або 1) або імовірнісний сигнал від системи, описаної в [9].

Кожному динамічному фактору впливу (S_k) експертами з інформаційної безпеки присвоюється ваговий коефіцієнт небезпеки (w_k), який відображає критичність цього фактору для загального стану безпеки.

2.2. Модель розрахунку вектора зважених оцінок подій. Для отримання єдиного показника поточної інтенсивності загроз обчислюється вектор зважених оцінок подій $V(t)$. Він відображає сумарну «вагу» всіх виявлених загроз за певний часовий інтервал *t*:

$$V(t) = \sum_{k=1}^{m} w_k \cdot S_k(t), \quad (2)$$

де m – загальна кількість ДФВ;

w_k – ваговий коефіцієнт небезпеки для *k*-го динамічного фактору;

$S_k(t)$ – поточне значення *k*-го динамічного фактору за часовий інтервал *t*.

Чим вище його значення, тим більший вплив негативних подій на безпеку.

Далі розраховується нормалізована оцінка впливу подій $\bar{Y}_{\text{подій}}(t)$ за часовий інтервал *t*:

$$\bar{Y}_{\text{подій}}(t) = \frac{V(t)}{V_{max}}, \quad (3)$$

де V_{max} – експертно визначений максимально можливий рівень загрози.

Для зручності інтерпретації (1 – краща безпека, 0 – відсутність безпеки) оцінка інвертується:

$$Y_{\text{подій}}(t) = 1 - \bar{Y}_{\text{подій}}(t). \quad (4)$$

Якщо $\bar{Y}_{\text{подій}}(t)$ перевищить 1 (тобто $V(t) > V_{max}$), що свідчить про надзвичайно високу активність загроз, то $Y_{подій}(t)$ може стати від'ємним, або його можна вважати нульовим.

Eman 3. Визначення загальної інтегральної оцінки ($Y_{загальна}$). На фінальному кроці фази динамічної оцінки відбувається інтеграція базової та динамічної оцінок для формування єдиного показника стану безпеки. Як комбінаційна функція використовується добуток, що дозволяє відобразити мультиплікативний ефект:

$$Y_{\text{загальна}}(t) = Y^{*}_{\text{базова}}(t) \times Y_{\text{подій}}(t). \quad (5)$$

Ця функція передбачає, що навіть якщо базова безпека висока ($Y_{базова} \to 1$), велика кількість поточних подій ($Y_{подій} \to 0$) значно знизить загальну оцінку, відображаючи реальне погіршення ситуації.

Отримане значення $Y_{загальна}(t)$ інтерпретується за допомогою порогових рівнів, на кшталт:

– нормальний: $Y_{загальна}(t) \geq 0{,}7$;
– попереджувальний: $0{,}5 \leq Y_{загальна}(t) < 0{,}7$;
– критичний: $Y_{загальна}(t) < 0{,}5$.

Отримана оцінка $Y_{загальна}(t)$ є не кінцевою метою, а тригером для адаптивного управління, що включає:

– моніторинг та порогові значення. Система безперервно обчислює $Y_{загальна}(t)$. Коли оцінка перетинає визначені пороги (наприклад, падає нижче 0,5, переходячи в «критичний» рівень), вона сигналізує про неприпустиме погіршення стану безпеки;

– запуск автоматизованих сценаріїв (SOAR). Сигнал від алгоритму передається на платформу оркестрації та автоматизації безпеки (SOAR). Залежно від того, які саме ДФВ (динамічні фактори від ШІ) спричинили падіння оцінки, запускається відповідний сценарій реагування (ізоляція хоста, блокування IP-адреси, посилення моніторингу);

– зворотний зв'язок та саморегуляція. Адаптація також передбачає вплив на сам алгоритм. Наприклад, якщо певний тип загрози (ДФВ) виникає постійно, система може автоматично збільшити його ваговий коефіцієнт w_k, роблячи загальну оцінку більш чутливою до цього вектора атак у майбутньому.

Таким чином, запропонований алгоритм створює замкнений цикл: ШІ-системи аналізують контент → Алгоритм агрегує їхні висновки в єдину оцінку → Оцінка запускає адаптивні дії → Дії змінюють середовище, що знову аналізується ШІ-системами. Саме це і є практичною реалізацією адаптивної безпеки.

Висновки. У статті вирішено актуальну наукову задачу розробки методологічного підходу до адаптивної оцінки стану безпеки мережевого контенту в умовах невизначеності, що спричинена динамікою сучасних кіберзагроз та різнорідністю даних.

У результаті дослідження розроблено алгоритм визначення агрегованої динамічної оцінки стану безпеки мережевого контенту. Його ключовою особливістю є триетапна структура, що комплексно поєднує статичні та динамічні аспекти безпеки:

Етап 1. Розрахунок нечіткої базової оцінки ($Y_{\text{базова}}$) за допомогою нелінійної нечіткої регресійної моделі, що дозволяє формалізувати та обробити експертні знання про фундаментальний рівень захищеності системи.

Етап 2. Розрахунок динамічної оцінки впливу подій ($Y_{\text{подій}}$), яка інтегрує кількісні показники, отримані безпосередньо від сучасних систем штучного інтелекту (ШІ), що аналізують мережевий контент у реальному часі.

Етап 3. Синтез базової та динамічної складових у єдиний інтегральний показник ($Y_{загальна}$), що слугує обґрунтованим індикатором поточного стану безпеки.

Наукова новизна запропонованого підходу полягає у створенні методу, який поєднує нелінійну нечітку модель для обробки статичних факторів із моделлю динамічної оцінки, що безпосередньо використовує висновки інтелектуальних систем аналізу. Це дозволяє формалізувати та автоматизувати процес агрегації різнорідних, неповних та неточних даних в єдиному фреймворку.

Практична цінність розробленого алгоритму полягає в тому, що він надає кількісну основу для переходу від реактивного до проактивного, ризик-орієнтованого управління безпекою. Отримана інтегральна оцінка є тригером для механізмів адаптивного реагування, зокрема для автоматизованих платформ (SOAR), що підвищує швидкість та ефективність протидії як відомим, так і раніше невідомим загрозам, посилюючи загальну стійкість.

Напрямками подальших досліджень є вдосконалення запропонованого алгоритму, що включає: розробку методів автоматичної адаптації функцій належності та калібрування нечітких коефіцієнтів (β) за допомогою машинного навчання; створення алгоритмів для динамічної оптимізації вагових коефіцієнтів (w_k); інтеграцію з системами аналізу поведінки користувачів (UEBA) та проведення повномасштабних експериментальних досліджень на реальних мережевих інфраструктурах.

Заява про використання генеративного ШІ та технологій на основі ШІ в процесі написання тексту статті

Для підвищення якості рукопису автори застосували інструменти на основі штучного інтелекту (зокрема, Chat GPT) з метою усунення стилістичних та граматичних помилок. Весь згенерований або модифікований контент був ретельно перевірений, відредагований та схвалений авторами, які несуть повну відповідальність за остаточний зміст публікації.

Список використаних джерел

1. Stouffer, K., Falco, J., & Scarfone, K. (2011). *Guide to Industrial Control Systems (ICS) Security* (NIST Special Publication 800-82). National Institute of Standards and Technology. https://www.researchgate.net/publication/308175656_NIST_Special_Publication_800-82_Guide_to_Industrial_Control_Systems_ICS_Security.

2. Homer, J., Zhang, S., Ou, X., & Schmid, D. (2013). Aggregating vulnerability metrics in enterprise networks using attack graphs. *Journal of Computer Security, 21*(4), 561-597. https://doi.org/10.3233/JCS-130475.

3. Barford, P., & Dacier, M. (Eds.). (2017). *Cyber–security metrics and performance measurement*. Springer. https://doi.org/10.1002/9780470087923.hhs440.

4. Zadeh, L. A. (1965). Fuzzy sets. *Information and Control, 8*(3), 338-353. https://doi.org/10.1016/S0019-9958(65)90241-X.

5. Lytvynov, V., Hrebennyk, A., Trunova, E., & others. (2021). *Principles of adaptive corporate network security management.* In S. Shkarlet, A. Morozov, & A. Palagin (Eds.), *Mathematical modeling and simulation of systems (MODS'2020)* (pp. 289-300). Cham: Springer. *(Advances in Intelligent Systems and Computing, Vol. 1265).* http://dwl.kiev.ua/art/spring20/mmss.pdf.

6. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security. *IEEE Communications Surveys & Tutorials, 18*(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502.

7. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 108-116. https://doi.org/10.5220/0006639801080116.

8. Brandão, P. (2025). Combating advanced persistent threats through artificial intelligence: An algorithmic approach. *Open Research Europe, 5*, Article 139. https://doi.org/10.12688/openreseurope.20268.2.

9. Albalawi, T., Ganeshkumar, P., & Albalwy, F. (2025). *Strategic network attack prevention system leveraging sophisticated query-based network attention algorithm (QNAA) and self-perpetuating generative adversarial network (SPF-GAN) techniques for optimal detection*. *Electronics, 14*(5), Article 922. https://doi.org/10.3390/electronics14050922.

10. Литвинов, В. В., Казимир, В. В., Стеценко, І. В., та ін. (2017). *Методи аналізу та моделювання безпеки розподілених інформаційних систем* (С. М. Шкарлет, ред.). Чернігівський національний технологічний університет.

11. Zadeh, L. A. (1994). Fuzzy logic, neural networks, and soft computing. *Communications of the ACM, 37*(3), 77-84. https://doi.org/10.1145/175247.175255.

12. Zadeh, L. A. (1996). Fuzzy logic = computing with words. *IEEE Transactions on Fuzzy Systems, 4*(2), 103-111. https://doi.org/10.1109/91.493904.

13. ISO/IEC. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. https://www.iso.org/standard/82875.html.

14. ISO/IEC. (2022). *ISO/IEC 15408-1:2022 – Information security, cybersecurity and privacy protection — Evaluation criteria for IT security – Part 1: Introduction and general model*. https://cdn.standards.iteh.ai/samples/72891/fbfa4f603f384c7ab0663ffc4c163f3f/ISO-IEC-15408-1-2022.pdf.

15. Korystin, O. Y., Korchenko, O., Kazmirchuk, S., et al. (2024). Comparative risk assessment of cyber threats based on average and fuzzy sets theory. *I. J. Computer Network and Information Security, 1*(1), 24-34. https://doi.org/10.5815/ijcnis.2024.01.02.

16. Trunov, O., Skiter, I., Dorosh, M., et al. (2024). Modeling of the information security risk of a transport and logistics center based on fuzzy analytic hierarchy process. In V. Kazymyr et al. (Eds.), *Mathematical modeling and simulation of systems. MODS 2023* (Lecture Notes in Networks and Systems, Vol. 1091, pp. 250-261). Springer. https://doi.org/10.1007/978-3-031-67348-1_23.

References

1. Stouffer, K., Falco, J., & Scarfone, K. (2011). *Guide to industrial control systems (ICS) security* (NIST Special Publication 800-82). National Institute of Standards and Technology. https://www.researchgate.net/publication/308175656_NIST_Special_Publication_800-82_Guide_to_Industrial_Control_Systems_ICS_Security.

2. Homer, J., Zhang, S., Ou, X., & Schmid, D. (2013). Aggregating vulnerability metrics in enterprise networks using attack graphs. *Journal of Computer Security*, *21*(4), 561-597. https://doi.org/10.3233/JCS-130475.

3. Barford, P., & Dacier, M. (Eds.). (2017). *Cyber-security metrics and performance measurement*. Springer. https://doi.org/10.1002/9780470087923.hhs440.

4. Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, *8*(3), 338-353. https://doi.org/10.1016/S0019-9958(65)90241-X.

5. Lytvynov, V., Hrebennyk, A., Trunova, E., Skiter, I., & Lysetskyi, Y. (2021). Principles of adaptive corporate network security management. In S. Shkarlet, A. Morozov, & A. Palagin (Eds.), *Mathematical modeling and simulation of systems (MODS'2020)* (pp. 289-300). Springer. http://dwl.kiev.ua/art/spring20/mmss.pdf.

6. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502.

7. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *Proceedings of the 4th International*

Conference on Information Systems Security and Privacy (ICISSP) (pp. 108-116). Scitepress. https://doi.org/10.5220/0006639801080116.

8. Brandão, P. (2025). Combating advanced persistent threats through artificial intelligence: An algorithmic approach. *Open Research Europe*, *5*, Article 139. https://doi.org/10.12688/openreseurope.20268.2.

9. Albalawi, T., Ganeshkumar, P., & Albalwy, F. (2025). Strategic network attack prevention system leveraging sophisticated query-based network attention algorithm (QNAA) and self-perpetuating generative adversarial network (SPF-GAN) techniques for optimal detection. *Electronics*, *14*(5), 922. https://doi.org/10.3390/electronics14050922.

10. Lytvynov, V. V., Kazymyr, V. V., Stetsenko, I. V., Trunova, O. V., Skiter, I. S., Tkach, Y. M., Hrebennyk, A. H., & Nekhay, V. V. (2017). *Metody analizu ta modeliuvannia bezpeky rozpodilenykh informatsiinykh system: monohrafiia [Methods of analysis and modeling of security of distributed information systems: A monograph].* Chernihiv National University of Technology.

11. Zadeh, L. A. (1994). Fuzzy logic, neural networks, and soft computing. Communications of the ACM, 37(3), 77-84. https://doi.org/10.1145/175247.175255.

12. Zadeh, L. A. (1996). Fuzzy logic = computing with words. IEEE Transactions on Fuzzy Systems, 4(2), 103-111. https://doi.org/10.1109/91.493904.

13. International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements* (ISO/IEC 27001:2022). https://www.iso.org/standard/82875.html.

14. International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model* (ISO/IEC 15408-1:2022). https://cdn.standards.iteh.ai/samples/72891/fbfa4f603f384c7ab0663ffc4c163f3f/ ISO-IEC-15408-1-2022.pdf.

15. Korystin, O. Y., Korchenko, O., Kazmirchuk, S., Demediuk, S., & Korystin, O. O. (2024). Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Sets Theory. *I. J. Computer Network and Information Security*, *1*(1), 24-34. https://doi.org/10.5815/ijcnis.2024.01.02.

16. Trunov, O., Skiter, I., Dorosh, M., Trunova, E., & Voitsekhovska, M. (2024). Modeling of the information security risk of a transport and logistics center based on fuzzy analytic hierarchy process. In V. Kazymyr, D. Peleshko, A. Morozov, & S. Shkarlet (Eds.), *Mathematical modeling and simulation of systems. MODS 2023* (pp. 250-261). Springer. https://doi.org/10.1007/978-3-031-67348-1_23.

Отримано 21.09.2025

UDC 004.056:004.8

Alla Hrebennyk[1], Oleksii Trunov[2]

[1]Senior Lecturer at the Department of Cybersecurity and Mathematical Modeling
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: grebennik.alla@gmail.com. **ORCID:** https://orcid.org/0000-0002-7464-1412
Scopus Author ID: 57219054928

[2]PhD student, Lecturer at the Department of Information Technology and Software Engineering
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: alexeytrunov1995@gmail.com. **ORCID:** https://orcid.org/0009-0002-0321-2669
Scopus Author ID: 59337119500T

THE ALGORITHM FOR DETERMINING THE AGGREGATED DYNAMIC ASSESSMENT OF THE SECURITY STATE OF NETWORK CONTENT

Amid the exponential growth of network content volume and the permanent evolution of cyber threats, traditional approaches to corporate network protection based on signature analysis are proving to be insufficient. A paradigm shift is occurring from static perimeter defense to continuous intelligent analysis of data streams. This brings to the forefront the problem of decision-making under significant uncertainty, caused by the heterogeneity, incompleteness, and imprecision of information coming from numerous security tools. Therefore, the development of a scientific and methodological apparatus for the comprehensive real-time assessment of the security state is an extremely urgent task that meets modern information security challenges.

The key scientific and practical problem is the absence of a unified, formalized methodology that would allow for a holistic assessment of the security state of network content. Existing security tools generate a large amount of unstructured data, but a mechanism for their aggregation into a single, interpretable indicator is lacking. The problem can be decomposed

into three components: 1) the problem of aggregating heterogeneous data, including static configuration parameters and dynamic verdicts from artificial intelligence systems; 2) the problem of ensuring the dynamism of the assessment for effective counteraction to adaptive, time-varying threats; 3) the problem of formalizing assessment criteria under fuzzy and incomplete input data, which requires the application of an appropriate mathematical apparatus.

The objective of this paper is to develop an algorithm for determining the aggregated dynamic assessment of the security state of network content. The proposed algorithm is intended to solve the aforementioned problems by acting as a fusion engine that synthesizes heterogeneous security indicators. It must provide a mechanism for quantifying the current level of security, considering both the fundamental reliability of the system and the current intensity of threats, and serve as a justified basis for triggering adaptive response mechanisms.

The proposed algorithm is implemented in three stages. In the first stage, a fuzzy base assessment (Y_{base}) is calculated, which reflects the static level of the system's security. This is achieved using a non-linear fuzzy regression model, with inputs being expert assessments of functional security criteria (in accordance with ISO 15408). In the second stage, a dynamic assessment of event impact (Y_{events}) is determined. Its inputs are dynamic influence factors (DIFs) – quantitative indicators generated by artificial intelligence systems (e.g., the probability of a phishing attack from an NLP model, the traffic anomaly level from a deep learning model). These indicators are weighted and normalized to obtain a single assessment of current threats. In the third stage, the base and dynamic assessments are integrated by multiplication ($Y_{total}(t) = Y^*_{base}(t) \times Y_{events}(t)$) to form the final aggregated indicator.

As a result of the research, a new scientific and methodological apparatus for assessing the security state of network content has been developed. The proposed algorithm formalizes the process of integrating heterogeneous, incomplete, and fuzzy data, combining static and dynamic aspects of security. Its key advantage is the ability to use the outputs of modern AI systems as input data, which allows for the consideration of previously unknown threats. The resulting aggregated dynamic assessment is a quantitative, interpretable indicator that can be used as a trigger for automated response systems (SOAR). This enables a shift from a reactive to a proactive security management paradigm, enhancing the overall resilience of network content against modern cyberattacks.

Keywords: *information security; network content; aggregated assessment; dynamic assessment; artificial intelligence; fuzzy logic; adaptive management.*

Fig.: 1. Table: 1. References: 16.

Гребенник А. Г., Трунов О. І. Алгоритм визначення агрегованої динамічної оцінки стану безпеки мережевого контенту. *Технічні науки та технології,* 2025. № 3(41). С. 158-168. DOI: https://doi.org/10.25140/2411-5363-2025-3(41)-158-168.