УДК 004.056.5:005.8 **DOI:10.30837/rt.2025.3.222.07**

Т.І. КОРОБЕЙНІКОВА, канд. техн. наук, А.Б. ЯМНИЧ

ПРОЦЕСНА МОДЕЛЬ ДИНАМІЧНОГО АНАЛІЗУ ТА ПРОГНОЗУВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПЕРСОНАЛУ

Вступ

Цифровізація бізнес-процесів, гібридні моделі роботи та зростання залежності від розподілених сервісів суттєво підвищили вагу людського фактора та персоналу зокрема в кіберзагрозах [1 – 3]. Традиційні періодичні процедури оцінювання ризиків та статичні політики доступу не встигають за динамікою середовища, де контекст доступу, рівень навантаження, поведінкові патерни користувачів і загальна загрозова картина змінюються у реальному (майже) часі [4 – 6]. Саме тому організаціям потрібні моделі, що поєднують безперервний моніторинг, динамічну оцінку ризику і негайне застосування контрзаходів, узгоджених з принципами Zero Trust [7, 8] та вимогами аудитованості й прозорості. Нормативні орієнтири (зокрема NIST SP 800-207) [9, 10] прямо підкреслюють необхідність відмови від «імпліцитної довіри» і переходу до рішень, що щоразу верифікують суб'єкта, пристрій і запитуваний ресурс з урахуванням контексту, ризику та політик організації [11, 12].

Запропонована у поданому тексті процесна модель акумулює ці потреби й тренди в єдину архітектуру: 1) формує багатовимірну матрицю класифікації ресурсів; 2) збирає технічні та поведінкові дані; 3) нормалізує їх у вектор ознак Q; 4) будує цифровий двійник користувача для прогнозування ризиків; 5) генерує адаптивні контрзаходи та навчальний контент; 6) доставляє персоналізовані політики доступу; 7) збирає результати впровадження; 8) самонавчається, коригуючи ваги, моделі та правила RBAC-блокчейну. Така інтеграція безпосередньо задовольняє актуальні запити ринку: оперативність, персоніфікацію, прозорість аудиту та стале підвищення кіберстійкості.

Метою роботи є підвищення точності та оперативності оцінювання ризиків інформаційної безпеки для персоналу, покращення керованості доступу через адаптивні політики на основі поведінкової аналітики та цифрових двійників, а також вдосконалення прозорості й відтворюваності аудиту за рахунок інтеграції RBAC-блокчейну в замкнений цикл самонавчання системи.

1. Аналіз останніх джерел в галузі ІБ в контексті діяльності компанії

Наукові огляди динамічного оцінювання ризику (Dynamic Risk Assessment, DRA) показують: статичні підходи не забезпечують потрібного рівня оперативності й точності у сучасних мережевих і хмарних середовищах; натомість моделі DRA інтегрують потоки подій (IDS/SIEM), контекстні атрибути та машинне навчання для безперервного перерахунку ризикових показників і суттєво підсилюють прийняття рішень щодо доступу й реагування [13].

Паралельно еволюціонують інструменти поведінкової аналітики (UEBA), що будують профілі користувачів і виявляють аномалії, зокрема для інсайдерських загроз – критичної категорії ризиків у корпоративному середовищі. Дослідження демонструють дієвість UEBA для безперервної автентифікації та виявлення девіацій у діях працівників і сервісів [14]. У промислових і кіберфізичних системах, де наслідки інсайдерської активності особливо дороговартісні, огляди підтверджують потребу в системних підходах до детекції, що поєднують технічні та поведінкові ознаки [15].

Ще один актуальний трендом є використання «цифрових двійників» (Digital Twins) для моделювання поведінки суб'єктів/систем і прогнозування небажаних сценаріїв. Сучасні огляди фіксують зрілість підходу та його релевантність саме до задач безпеки: симуляція сценаріїв, оцінювання вразливостей, прогнозування ризикових подій і тестування політик до їхнього застосування у кінцевих продуктах [16].

Нарешті, для вимог незмінності журналів доступу, відтворюваності аудиту й довіри між підсистемами зростає роль блокчейн-парадигм у контролі доступу (RBAC/ABAC із реєстра-

цією транзакцій доступу в розподіленому реєстрі). Систематичні огляди підтверджують потенціал блокчейну підвищувати довіру, прослідковуваність і автоматизацію політик, включно зі смарт-контрактами та ризик-адаптивними правилами [17 – 20].

Динамічне оцінювання ризику (DRA). Систематичний огляд Cheimonidis & Rantos (2023) узагальнює 50 моделей DRA і показує, що в сучасних умовах статичні процедури не забезпечують потрібної гнучкості [3]; провідні підходи використовують потоки подій (IDS), вразливості (NVD) і ML/BN для перерахунку ризику в (майже) реальному часі. Автори також підкреслюють потребу поєднувати DRA з розвідданими (CTI) та працювати у Zero Trust-контексті. Це добре корелює з місцем модуля f_4 (прогнозування) та f_8 (самонавчання) у запропонованій моделі.

Zero Trust і ризик-адаптивний контроль доступу. NIST SP 800-207 формулює перехід від периметрових припущень довіри до постійної верифікації суб'єктів, активів і запитів на доступ із урахуванням контексту, що підтримує ідею ризик-адаптивних політик (f_5 –f_6). Додатково SP 800-207A моделює архітектуру доступу у ZTA та демонструє, як будувати рішення з тонким урахуванням ризику у каналі прийняття рішень [1].

UEBA та інсайдерські загрози. На рівні поведінкових ознак сучасні праці підтверджують ефективність UEBA для безперервної автентифікації і виявлення аномалій. Martín et al. (2022) [4] у Knowledge-Based Systems показали, що комбінування клавіатурної та мишкової динаміки дає стійкі сигнали для безперервної автентифікації і це відповідає нашій функції f_2 –f_3 (збір/нормалізація) та побудові вектора Q. Для контексту загроз у CPS, де інсайдери особливо небезпечні, систематичний огляд (Computers & Electrical Engineering, 2024) показує прогалини у виявленні і підкреслює потребу мультиджерельних поведінкових і технічних сигналів і саме те, що робить запропонована ПМ.

Цифрові двійники у безпеці. Огляд IEEE Communications Surveys & Tutorials (Alcaraz & Lopez, 2022) систематизує загрози та контрзаходи для DT і підкреслює їхню корисність для моделювання та «what-if» аналізу безпеки. У нашій ПМ цифровий двійник користувача (f_4) симулює поведінку в штатних та аномальних сценаріях і генерує матрицю ймовірностей атак R, тобто підхід, що резонує з висновками огляду про прогностичну цінність DT [6].

Блокчейн-підсилення контролю доступу. Огляди й систематичні рев'ю [7 – 10] демонструють зрілість інтеграції блокчейну з ABAC/RBAC для підвищення довіри, незмінності логів і автоматизації політик (смарт-контракти, аудит, децентралізація). Для IoT/хмар показано класифікації парадигм доступу, сценарії застосування та виклики (масштабованість, приватність, продуктивність), що робить відстежуваність транзакцій доступу в нашому RBAC-блокчейні (f_4 , f_8) технічно обґрунтованою й методично захищеною.

Таким чином, поточна наукова картина підтверджує необхідність DRA у ZTA-рамці, дієвість UEBA для профілювання персоналу, прогностичну користь цифрових двійників, доречність блокчейну для незмінного аудиту та розподіленого управління політиками доступу. У сукупності це створює надійне підґрунтя для запропонованої процесної моделі з замкненим контуром самонавчання.

2. Процесна модель динамічного аналізу та прогнозування ризиків інформаційної безпеки для персоналу

У сучасних системах інформаційної безпеки (ІБ) основним елементом є персонал, водночас ефективність технічного захисту безпосередньо залежить від дій користувачів. Особливо це прослідковується під час контролю доступу до інформаційних ресурсів, де рішення про надання прав мають ґрунтуватися на об'єктивних критеріях: посаді, функціональних обов'язках, рівні відповідальності та контексті використання даних. Такий підхід забезпечує формалізовану та перевірену основу для визначення допустимого рівня доступу, перетворюючи довіру з абстрактного поняття на вимірюваний параметр в управлінні ризиками.

Таким чином, виникає потреба у розробці технологічних етапів динамічного аналізу та прогнозування ризиків інформаційної безпеки для персоналу, де рівень довіри визначається

через систему конкретних показників. Реалізація такої процесної моделі дає змогу автоматично формувати та модифікувати політики доступу на основі динамічного аналізу багатовимірного вектора ознак Q, що поєднує технічні та поведінкові параметри користувача з контекстом взаємодії з ресурсами. Оновлення прав відбувається в режимі реального часу із застосуванням алгоритмів прогнозування на основі цифрового двійника (f_4), тоді як RBAC-блокчейн гарантує криптографічно захищену реєстрацію кожної транзакції доступу в розподіленому реєстрі. Така архітектура дає змогу оперативно змінювати права відповідно до виявлених аномалій, і водночас гарантує верифікованість усіх змін доступу, мінімізуючи ризики несанкціонованих модифікацій.

Запропонована процесна модель (ПМ) динамічного аналізу та прогнозування ризиків інформаційної безпеки для персоналу: від збору даних до їхньої аналітичної обробки та прийняття рішень. Подана ПМ складається із процесів, і кожен з них відповідає за конкретну дію або процедуру. Така побудова дає системі необхідну гнучкість і здатність адаптуватися до реальних загроз, що виникають у повсякденній роботі з людьми, а не лише в межах теоретичних сценаріїв (рис. 1).

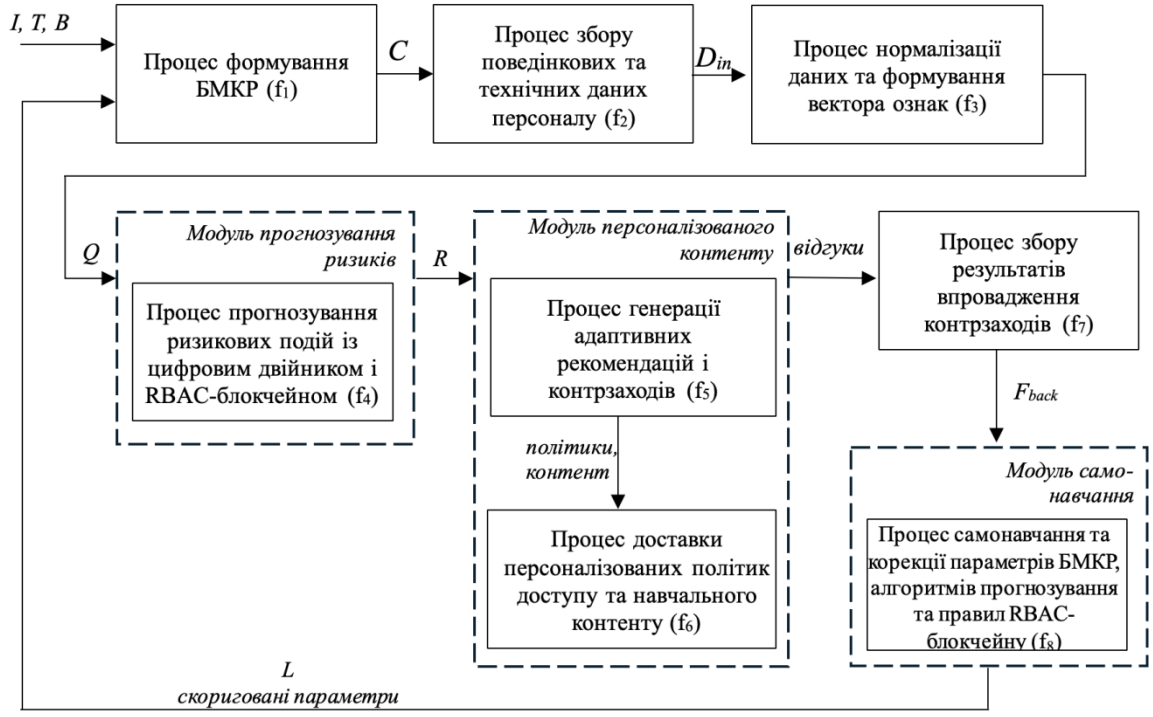

Рис. 1. Процесна модель динамічного аналізу та прогнозування ризиків інформаційної безпеки для персоналу

У запропонованій ПМ з персоніфікованим підходом дані поетапно перетворюються на адаптивні управлінські рішення, спрямовані на підвищення рівня захисту інформаційних ресурсів.

Процес формування багатовимірної матриці класифікації ресурсів.

На етапі формування багатовимірної матриці класифікації ресурсів (функція f_1) інформаційні ресурси структуруються за визначеними ознаками, серед яких можуть бути конфіденційність, цінність, доступність тощо. Вхідними даними для процесу формування БМКЛ є множини: I – інформаційні ресурси, T – технічні параметри і B – поведінкові метрики персоналу. Кожна ознака має вагу, яка показує її значущість у загальній системі. Методика відповідає підходам [22], заснованим на багатовимірному аналізі та експертному оцінюванні.

Процес збору поведінкових та технічних даних персоналу.

Процес збору поведінкових та технічних даних персоналу (функція f_2) передбачає збір та обробку даних C про поведінкову та технічну активність персоналу від БМКР. Джерелами

таких даних є журнали подій (логи), телеметричні показники, результати анкетування або тестування користувачів.

Процес нормалізації даних та формування вектора ознак.

В результаті роботи процесу нормалізації даних та формування вектора ознак (за функцією f_3) зібрані дані (нормалізовані та уніфіковані) формують вектор ознак Q. Цей вектор є формалізованим представленням поведінкових характеристик окремого суб'єкта доступу та використовується як вхідна змінна для подальших обчислень. Побудова вектора Q ґрунтується на поєднанні класичних статистичних методів і сучасних алгоритмів машинного навчання. Такий підхід відповідає рекомендаціям ризик-менеджменту в інформаційній безпеці.

Процес прогнозування ризикових подій із цифровим двійником і RBAC-блокчейном.

Процес прогнозування ризикових подій із цифровим двійником і RBAC-блокчейном (функція f_4) передбачає, що після формування вектора Q дані надходять до модуля прогнозування, де створюється так званий цифровий двійник користувача (ЦДК) – персоніфікована математична модель, що симулює його поведінку в умовах, наближених до реальних. ЦДК дає змогу оцінювати поточну активність і прогнозувати потенційні небажані дії. Модель ЦДК інтегрується з системами рольового контролю доступу (RBAC) та блокчейном, який фіксує дії користувача в незмінному реєстрі. Зазначені підходи обґрунтовано в дослідженнях із контролю доступу та застосування технологій блокчейн [20, 21].

На основі результатів симуляції формується матриця ймовірностей атак (R). Вона оцінює ймовірність різних типів порушень інформаційної безпеки конкретним користувачем щодо певних ресурсів.

Процес генерації адаптивних рекомендацій і контрзаходів та процес доставки персоналізованих політик доступу та навчального контенту є складовими Модуля персоналізованого контенту.

Модуль персоналізованого контенту передбачає, що на основі матриці R система генерує персоналізовані управлінські рішення, зокрема: адаптивні політики доступу, рекомендації щодо дій користувача (процес генерації адаптивних рекомендацій і контрзаходів за функцією f_5); а також навчальні матеріали з підвищення інформаційної грамотності (процес доставки персоналізованих політик доступу та навчального контенту за функцією f_6).

Процес збору результатів впровадження контрзаходів.

Заходи реалізуються (за функцією f_7) через інтерфейс взаємодії з користувачем, після чого активується модуль зворотного зв'язку. Його функція – моніторинг ефективності впроваджених рішень та збір коригувальних даних (F_{back}).

Процес самонавчання та корекції параметрів БМКР, алгоритмів прогнозування та правил RBAC-блокчейну.

Система використовує ці дані для самонавчання (за функцією f_8): оновлює вагові коефіцієнти, удосконалює прогнозні моделі та уточнює політики доступу. Отже, система працює як замкнутий адаптивний контур управління безпекою з персоналізованим оцінюванням ризиків.

Ідея, що лежить в основі запропонованої системи оцінювання ризиків інформаційної безпеки, полягає в комплексній інтеграції традиційних і сучасних методологічних підходів. Йдеться про поєднання класичних статистичних методів, алгоритмів машинного навчання, моделей цифрової поведінки користувачів і технологій блокчейн. Такий гібридний підхід поєднує реактивну та проактивну стратегії: система не лише фіксує загрози, а й заздалегідь прогнозує потенційні ризики.

Зокрема, упровадження блокчейн-технологій у цю систему виконує критично важливу функцію забезпечення цілісності та незмінності логів доступу до інформаційних ресурсів. Оскільки записи в блокчейні не підлягають редагуванню без фіксації цифрового сліду, це створює прозору, верифіковану історію взаємодії користувача із системами. Така незмінність підвищує рівень довіри до механізмів аудиту й сприяє обґрунтованому ухваленню рішень у контексті ризик-менеджменту. Фактично йдеться про формування надійного джерела даних

у цифровому середовищі, що є особливо важливим в умовах багаторівневої корпоративної інфраструктури.

3. Складові процесної моделі динамічного аналізу та прогнозування ризиків інформаційної безпеки для персоналу

На першому етапі відбувається процес формування матриці класифікації ресурсів (функція f_1) і слугує методологічною основою всієї системи. Побудова матриці передбачає аналіз наявних в організації інформаційних активів для їхнього структурованого опису за низкою релевантних ознак, серед яких технічна цінність ресурсу, його критичність для бізнес-процесів, рівень конфіденційності та контекст використання. Вагові коефіцієнти призначаються на основі комбінованого підходу, що поєднує елементи експертного оцінювання (із залученням фахівців з інформаційної безпеки, аналітиків і керівників підрозділів) та статистичні методи, такі як кореляційний аналіз або метод головних компонент (PCA, Principal component analysis), що мінімізує суб'єктивність. Принцип адаптації матриці полягає в періодичному перерахунку вагових коефіцієнтів зі зміною структури підприємства, складу інформаційних ресурсів або бізнес-процесів. Це реалізується через повторне застосування обраної методики вагового аналізу до оновленого набору ознак, що гарантує актуальність матриці щодо поточної організаційної конфігурації.

Другим етапом є процес збору й уніфікації поведінкових та технічних даних персоналу, позначений функцією f_2 . Його метою є формування повного та релевантного масиву даних, що відображає реальну активність користувачів у цифровому середовищі організації. Збір інформації відбувається з різних джерел: журнали подій серверів і прикладного ПЗ, телеметричні дані з мережевого обладнання, результати анкетування та опитувань, показники продуктивності праці. Отримані дані проходять обробку для очищення, нормалізації та синхронізації з урахуванням видалення дублікатів, виправлення форматних помилок та вирівнювання часових міток. Для уніфікації застосовуються формати CEF, JSON, LEEF, а передача між модулями відбувається через захищені канали (TLS).

На етапі роботи процесу нормалізації даних та формування вектора ознак f_3 виконується формування вектора ознак Q – числового представлення профілю користувача, що забезпечує його подальший аналіз математичними моделями. Формалізовано, $Q = \{x_1, x_2, \ldots, x_n\}$, де кожен x_i є нормалізованим і, за потреби, закодованим показником, отриманим із поведінкових чи технічних характеристик. На цьому етапі числові змінні масштабуються (Min–Max або z-нормалізація), а категоріальні – кодуються (one-hot encoding). Для кожної ознаки розраховуються статистичні характеристики (середнє, медіана, стандартне відхилення, коефіцієнт варіації, частота подій), після чого за допомогою Random Forest Feature Importance відбираються найбільш інформативні параметри. Отже, f_2 виконує збір даних, а f_3 перетворює їх у стандартизовану форму Q для моделювання.

Процес прогнозування ризикових подій із цифровим двійником і RBAC-блокчейном використовує функцію f_4 . Вектор Q надходить на вхід модуля прогнозування ризиків, де будується цифровий двійник працівника, який моделює його поведінку в штатних і потенційно аномальних сценаріях. У результаті формується матриця ймовірностей ризиків R, де кожен елемент відображає ймовірність реалізації певної загрози щодо конкретного інформаційного активу.

Функція f_5 процесу генерації адаптивних рекомендацій і контрзаходів має чітку мету – трансформувати матрицю R у набір конкретних контрзаходів, спрямованих на зниження ризиків, з урахуванням їхніх категорій та порогових значень. Розрізняють три категорії контрзаходів: превентивні (запобігають інциденту), детективні (виявляють його) та коригувальні (усувають наслідки). Активація відбувається, якщо ймовірність у R перевищує визначений поріг P^t, який налаштовується залежно від класу активу та допустимого рівня ризику (наприклад, $P^t = 0{,}7$ для критичних систем, 0,5 – для середньої важливості та 0,3 – для менш важливих). Якщо ризик перевищує поріг, запускаються адаптивні дії: від додаткової багато-

факторної автентифікації та тимчасового обмеження доступу до призначення обов'язкової ручної перевірки. Паралельно формується персоналізована програма підвищення обізнаності співробітника з питань кібербезпеки, контент якої динамічно адаптується до його актуального профілю ризику.

Таким чином, система усуває поточні загрози й знижує ризики в довгостроковій перспективі завдяки розвитку цифрової компетентності та кіберграмотності персоналу. Це створює додатковий рівень стійкості інформаційної системи підприємства, заснований на проактивному управлінні впливом діяльності людини.

Після того як система сформувала рекомендації з управління ризиками та навчальні матеріали для підвищення обізнаності користувачів, наступним етапом є процес доставки персоналізованих політик доступу та навчального контенту (що забезпечується функцією f_6) для ефективного доставлення цього контенту безпосередньо до кінцевих суб'єктів. Цей процес виконує Модуль персоналізованого контенту.

Функціонування цього модуля ґрунтується на мультиканальному підході до комунікації. Кожен користувач бачить персоналізовану інформаційну панель, адаптовану не лише до його ролі в організації, але й до виявлених ризиків. Інтерфейс структуровано так, щоб акцентувати на пріоритетних діях, зокрема на завданнях, які потребують негайного виконання, термінах їхнього завершення, способах підтвердження тощо. Такий підхід мінімізує часовий лаг між отриманням інформації та діями користувача, що зменшує «вікно ризику» – період, упродовж якого вразливість може бути використана.

В результаті роботи функції f_7 активується процес збору результатів впровадження контрзаходів, що збирає та аналізує реакцію користувача на отриманий контент і рекомендації. Мета цього етапу – не лише зафіксувати факт взаємодії, а й оцінити її якість, повноту та наслідки для зміни поведінки або рівня ризику.

Крім об'єктивних цифрових показників процес збору результатів впровадження контрзаходів використовує інструменти якісного аналізу: міні опитування, анкетування щодо зручності та зрозумілості контенту, а також відкриті поля для фідбеку. Інформація структурується та агрегується в матрицю зворотного зв'язку F_{back}, що містить кількісні (наприклад, середній час реагування) та якісні дані (наприклад, задоволеність користувача освітнім процесом). Це дає змогу виявляти не лише технічні уразливості, а й елементи культури безпеки в межах організації, зокрема мотивацію працівників, ступінь залученості та рівень цифрової відповідальності.

Останнім, але концептуально найважливішим компонентом системи є модуль самонавчання (функція f_8), завданням якого є динамічна адаптація всієї системи на основі даних, накопичених у матриці F_{back}. Це означає, що система не лише фіксує реакцію користувачів на застосовані контрзаходи, але й використовує цю інформацію для корекції власних моделей і правил.

Процес самонавчання та корекції параметрів БМКР, алгоритмів прогнозування та правил RBAC-блокчейну починається зі збору прикладів успішних і помилкових спрацювань прогнозної моделі (зокрема, випадків хибнопозитивних та хибнонегативних класифікацій). Для оцінювання якості моделі використовується функція втрат L, яка є зваженою комбінацією Binary Cross-Entropy та Focal Loss. Такий підхід дає змогу приділити увагу рідкісним, але критично важливим класам загроз, мінімізуючи при цьому кількість помилкових спрацьовувань.

Після обчислення L модуль f_8 ініціює процедуру автоматичного перенавчання, застосовуючи алгоритми глибокого навчання. Якщо аналіз матриці помилок свідчить про значний відсоток хибнопозитивних спрацювань для певної категорії подій, система коригує ваги ознак у багатовимірній матриці класифікації ресурсів (подає їх на вхід функції f_1) та оновлює відповідні RBAC-правила, знижуючи чутливість для цієї категорії. Якщо ж домінують хибнонегативні випадки, навпаки, вага підвищується, а політики доступу посилюються.

Механізм корекції RBAC-правил реалізується через модифікацію контекстних умов (наприклад, обмеження часу чи геолокації доступу) та рівнів авторизації (додавання або вилучення вимоги багатофакторної автентифікації). Усі зміни фіксуються в блокчейн-журналі доступу, що гарантує прозорість і неможливість несанкціонованого редагування політик.

Параметри моделі ризиків оновлюються двома способами: повним перенавчанням або частковим донавчанням (fine-tuning) із застосуванням підходу transfer learning, що дає змогу зберегти вже накопичені знання та швидко адаптувати модель до нових умов без значних обчислювальних витрат. Таким чином, функція f_8 виконує роль замикального механізму зворотного зв'язку, що підвищує точність та адаптивність системи в динамічному середовищі загроз.

Отже, повний цикл, від генерації контенту до отримання зворотного зв'язку й самокорекції, формує адаптивне середовище керування інформаційними ризиками, здатне оперативно реагувати на нові загрози, забезпечуючи гнучкість і стійкість системи. Інтеграція блокчейн-механізмів і класичних підходів до контролю доступу гарантує прозорість, верифікованість і захищеність усіх транзакцій та змін у системі. Така циклічна структура з елементами самонавчання й користувацької взаємодії забезпечує не просто стабільність, а еволюційний розвиток системи, що є критично важливим у динамічному середовищі інформаційної безпеки.

Висновки

Запропонована процесна модель адресує ключові виклики сучасної ІБ: динаміку загроз, вагу людського фактора, потребу в персоналізації й аудитованості. Завдяки поетапній трансформації даних у вектор ознак Q, побудові цифрового двійника користувача та матриці ризиків R, а також модулю персоналізованого контенту й механізму самонавчання система забезпечує підвищення точності оцінювання ризику, покращення оперативності реагування через ризик-адаптивні політики доступу та вдосконалення прозорості змін і журналів за рахунок RBAC-блокчейну. Порівняння з сучасними підходами (DRA/UEBA/ZTA/блокчейн-АС) підтверджує методологічну узгодженість і практичну релевантність моделі для корпоративних середовищ, зокрема там, де критичною є відтворюваність аудиту та стале зниження інсайдерських ризиків.

Список літератури:

1. Papanikolaou A., Varvarousi E., & Gavala E. Postal sector digitalisation: Security and vulnerabilities // International Journal of Applied Systemic Studies. 2024. 11(1). P. 42–51. https://doi.org/10.1504/IJASS.2024.139211(inderscience.com).

2. Sèdes F., & Degrace J. (2024). Social engineering and security: From human vulnerabilities to malicious threats // 20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). 2024. P. 301–305. IEEE. https://doi.org/10.1109/WiMob61911.2024.10770451.

3. Marushchak L., Pavlykivska O., Khrapunova Y., Kostiuk V., & Berezovska L. The economy of digitalization and digital transformation: Necessity and payback11th International Conference on Advanced Computer Information Technologies (ACIT). 2021. P. 305–308. IEEE. https://doi.org/10.1109/ACIT52158.2021.9548529.

4. Alnafea F. S. M., Sengar A. S., Hamid N. K., Selladurai K. M., Hassan S. I., & Saravanakumar R. Improving multi-factor authentication security with deep learning-based user behaviour analysis // 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS). 2025. P. 1–5. IEEE. https://doi.org/10.1109/ICICACS65178.2025.10968961.

5. Kaur M., & Garg P. Exploring behavioral patterns for security in cloud computing: A case study // 3rd International Conference on Advancement in Computation & Computer Technologies (InCACCT). 2025. P. 720–725. IEEE. https://doi.org/10.1109/InCACCT65424.2025.11011337.

6. Terumalasetti S., & Reeja S. R. Enhancing social media user's trust: A comprehensive framework for detecting malicious profiles using multi-dimensional analytics // IEEE Access. 2025. Vol. 13. P. 7071–7093. https://doi.org/10.1109/ACCESS.2024.3521951.

7. Korobeinikova T. I. The zero trust model: Theory, practice, and prospect. In Heritage of European Science 2025: Innovative technology, computer science, cybernetics and automation, security systems, transport development, architecture and construction, physics and mathematics (Monographic series "European Science," Book 37, Part 1, pp. 126–147). European Science. ISBN 978-3-98924-080-3.

8. Коробейнікова Т., Журавель І., Бодак А., & Бороденко Д. Концепція нульової довіри: сучасні методи забезпечення кібербезпеки в корпоративних мережах // Вісник Львів. держ. ун-ту безпеки життєдіяльності. 2025. Т. 30. С. 67–77. Retrieved із https://journal.ldubgd.edu.ua/index.php/Visnuk/article/view/2769.

9. Lee S., Huh J.-H., & Woo H. Security System Design and Verification for Zero Trust Architecture. Electronics. 2025. Vol. 14(4). P.643. https://doi.org/10.3390/electronics14040643.

10. Molina M., Betarte G., & Luna C. Consent validation for personal data access control using ABAC // Proceedings of the 13th Latin-American Symposium on Dependable and Secure Computing (LADC '24). 2024. P. 30–31. Association for Computing Machinery. https://doi.org/10.1145/3697090.3699803.

11. Rose S., Borchert O., Mitchell S., & Connelly S. Zero Trust Architecture (NIST Special Publication 800-207) // National Institute of Standards and Technology. 2020. https://doi.org/10.6028/NIST.SP.800-207.

12. Chandramouli R., Badger L., & O'Rourke D. SP 800-207A: A Zero Trust Architecture Model for Access Control in Cloud-Native Applications. NIST. 2023. https://csrc.nist.gov/pubs/sp/800/207/a/final (csrc.nist.gov).

13. Cheimonidis P., & Rantos K. Dynamic risk assessment in cybersecurity: A systematic literature review // Future Internet. 2023. Vol. 15(10). P. 324. https://doi.org/10.3390/fi15100324 (MDPI).

14. Martín A. G., Martín-de-Diego I., Fernández-Isabel A., et al. Combining user behavioural information at the feature level to enhance continuous authentication systems // Knowledge-Based Systems. 2022. Vol. 244. P. 108544. https://doi.org/10.1016/j.knosys.2022.108544 (ScienceDirect).

15. Al-Mhiqani M. N., Alsboui T. A. A., Al-Shehari T., Abdulkareem K. H., et al. Insider threat detection in cyber-physical systems: A systematic literature review // Computers & Electrical Engineering. 2024. Vol. 119, P. 109489. https://doi.org/10.1016/j.compeleceng.2024.109489 (ResearchGate).

16. Alcaraz C., & Lopez J. Digital twin: A comprehensive survey of security threats // IEEE Communications Surveys & Tutorials. 2022. Vol. 24(3). P. 1475–1503. https://doi.org/10.1109/COMST.2022.3171465 (NICS Lab).

17. Ullah S. S., Oleshchuk V., & Pussewalage H. S. G. A survey on blockchain-envisioned attribute-based access control for Internet of Things: Overview, comparative analysis, and open research challenges // Computer Networks. 2023. Vol. 235. P. 109994. https://doi.org/10.1016/j.comnet.2023.109994 (ACM Digital Library).

18. Punia A., Hoda M., Kaushik K., & Tomar D. A systematic review on blockchain-based access control systems in cloud environment // Journal of Cloud Computing. 2024. Vol. 13. P. 62. https://doi.org/10.1186/s13677-024-00697-7(PMC).

19. Namane S., Derhab A., Guerroumi M., & Challal Y. Blockchain-based access control techniques for IoT: A systematic review // Electronics. 2022. Vol. 11(14). P. 2225. https://doi.org/10.3390/electronics11142225 (MDPI).

20. Ямнич А. Б. Модель контролю доступу персоналу до інформаційних ресурсів підприємств на основі RBAC та технології BLOCKCHAIN / А.Б. Ямнич, Т.І. Коробейнікова // Вісник Хмельниц. нац. ун-ту. 2024. Т. 343, №6(1). С. 380–386. ISSN 2307–5732 https://doi.org/10.31891/2307-5732-2024-343-6-56.

21. Коробейнікова Т. І. Багатовимірна матриця класифікації інформації для оцінки ризиків інформаційної безпеки / Т. І. Коробейнікова, А. Б. Ямнич // Інформаційні технології та комп'ютерна інженерія. 2024. №2. С. 91–106. ISSN 1999–9941.

22. Korobeinikova T., Tachenko I., Romanyuk O., Romanyuk S., Stakhov O. and Reyda O. Assessing Network Security Risks: a Technological Chain Perspective // 14th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic. 2024. P. 565–570.
doi: 10.1109/ACIT62333.2024.10712586.

Надійшла до редколегії 03.06.2025

Відомості про авторів:

Коробейнікова Тетяна Іванівна – канд. техн. наук, Національний університет «Львівська політехніка», доцент кафедри безпеки інформаційних технологій; Україна; e-mail: tetianakorobeinikova@gmail.com; ORCID: https://orcid.org/0000-0003-2487-8742

Ямнич Андрій Богданович – Національний університет «Львівська політехніка», аспірант кафедри безпеки інформаційних технологій; Україна; e-mail: andrii.b.yamnych@lpnu.ua; ORCID: https://orcid.org/0009-0005-7226-1896