КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1364
УДК 004.056.5:004.7

Сидоренко Вікторія Миколаївна
к.т.н., доцент, доцент кафедри комп'ютерних інформаційних технологій
Національний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Кобільник Богдан Юрійович
аспірант факультету комп'ютерних наук та технологій
Національний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0009-0001-4848-541X
2539821@stud.kai.edu.ua

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ АДАПТИВНОЇ МОДЕЛІ КОНТЕКСТНОГО КОНТРОЛЮ ДОСТУПУ ДЛЯ ПІДВИЩЕННЯ СТІЙКОСТІ КРИТИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація. У сучасних умовах зростання кількості та складності кіберзагроз забезпечення безпечного доступу до критичних інформаційних систем (КІС) є одним із важливих завдань захисту критичної інформаційної інфраструктури держави. Особливої актуальності набуває застосування адаптивних механізмів контролю доступу, здатних враховувати зміну технічного стану кінцевого пристрою, рівня привілеїв користувача та параметрів середовища доступу відповідно до принципів архітектури Zero Trust. У статті представлено експериментальне дослідження адаптивної моделі контекстного контролю доступу для підвищення стійкості КІС. Для проведення експерименту конкретизовано параметри моделі з урахуванням особливостей КІС енергетичного сектору, сформовано множину сценаріїв доступу та реалізовано програмне оцінювання ефективності запропонованого підходу порівняно з відомими моделями контролю доступу. Отримані результати експериментального дослідження підтвердили адекватність та працездатність запропонованої моделі, а також її здатність адаптивно формувати рішення щодо доступу з урахуванням зміни контекстних параметрів. Для сценаріїв, пов'язаних із технічним станом кінцевого пристрою, модель продемонструвала найвище середнє значення точності серед досліджуваних підходів – 0,742, а за еталонної політики з пріоритетним урахуванням технічного стану пристрою точність становила 0,756. Результати дослідження підтвердили доцільність застосування запропонованої моделі для КІС, у яких технічний стан кінцевого пристрою є одним із пріоритетних факторів ризику. Практичне значення отриманих результатів полягає у можливості застосування розробленої моделі для побудови адаптивних систем контекстного контролю доступу до КІС з урахуванням профілю загроз конкретного об'єкта критичної інформаційної інфраструктури. Подальші дослідження будуть спрямовані на вдосконалення способу агрегування контекстних параметрів, розширення множини експериментальних сценаріїв та апробацію запропонованої моделі на реальних даних КІС.

Ключові слова: критичні інформаційні системи; критична інфраструктура; контекстний контроль доступу; адаптивна модель; Zero Trust; оцінювання ризику; кібербезпека; стійкість.

ВСТУП

Постановка проблеми. Критичні інформаційні системи (КІС) [1] будь якого сектору функціонують в умовах постійного зростання кількості та складності кіберзагроз, що в сучасних умовах можуть поєднуватися з фізичними та іншими дестабілізуючими впливами. Одним із важливих завдань забезпечення захищеності та стійкості таких систем є організація контролю доступу до їх інформаційних і технологічних ресурсів. Традиційні механізми контролю доступу, зокрема рольові та атрибутні, переважно ґрунтуються на наперед визначених правилах і не завжди враховують динамічні характеристики конкретного запиту. До таких характеристик належать технічний стан кінцевого

пристрою, рівень привілеїв користувача, параметри мережевого середовища, місце та умови здійснення доступу. За таких умов формально легітимний запит може становити загрозу для КІС у разі використання скомпрометованого або некерованого пристрою, аномального середовища доступу чи облікового запису з підвищеним рівнем привілеїв.

Урахування зазначених чинників потребує переходу від статичних механізмів авторизації до адаптивного контекстного контролю доступу, за якого рішення щодо надання, обмеження або блокування доступу формується з урахуванням поточного рівня ризику. Одним із сучасних підходів до реалізації такого принципу є архітектура Zero Trust [2], [3], яка передбачає постійне оцінювання довіри та перевірку параметрів кожного запиту доступу. Водночас практичне застосування принципів Zero Trust у КІС потребує розроблення формалізованих моделей, що забезпечують кількісне оцінювання контекстних параметрів, визначення рівня ризику запиту та формування відповідного рішення щодо доступу. Необхідність розвитку таких підходів підтверджується сучасними нормативними вимогами та тенденціями кібербезпеки. Директива ЄС 2022/2555 (NIS2) визначає управління ідентичністю та доступом, багатофакторну автентифікацію, захист і належне конфігурування кінцевих пристроїв серед важливих заходів управління ризиками кібербезпеки [5]. Аналогічні принципи щодо застосування архітектури Zero Trust для захисту критичної інфраструктури представлені у рекомендаціях CSA [4]. Актуальність урахування контексту доступу підтверджується також статистикою сучасних кіберінцидентів. За даними ENISA, об’єкти критичної інфраструктури та промислові системи керування залишаються одними з пріоритетних цілей кіберзагроз [6]. У звіті Verizon DBIR 2025, сформованому на основі 22 052 інцидентів та 12 195 підтверджених витоків даних, зазначено значну роль компрометації облікових даних, експлуатації вразливостей та використання некерованих пристроїв у реалізації атак [7]. Це підтверджує доцільність урахування технічного стану пристрою, рівня автентифікації та параметрів середовища під час оцінювання ризику запиту доступу.

Особливої актуальності зазначена проблема набуває для КІС енергетичного сектору України. Так, у 2024 р. CERT-UA зафіксовано цілеспрямовані атаки угруповання UAC-0133 (Sandworm) на об’єкти енерго-, водо- та теплопостачання, під час яких одним із шляхів отримання первинного доступу стало використання скомпрометованих ланцюгів постачання та технічних можливостей персоналу постачальників щодо віддаленого доступу до інформаційно-комунікаційних систем [8]. Скомпрометовані обчислювальні засоби при цьому належали, зокрема, до контурів автоматизованих систем управління технологічними процесами, що підтверджує необхідність посилення контролю віддаленого, адміністративного та підрядного доступу до КІС енергетичного сектору.

Таким чином, актуальним науково-прикладним завданням є експериментальне дослідження адаптивної моделі контекстного контролю доступу, яка на основі комплексного врахування технічного стану пристрою, рівня привілеїв користувача та параметрів середовища забезпечує оцінювання ризику запиту й формування відповідного рішення щодо доступу до ресурсів КІС.

Аналіз останніх досліджень і публікацій. У попередній роботі авторів [9] запропоновано адаптивну модель контекстного контролю доступу до КІС, яка передбачає комплексне врахування трьох груп контекстних параметрів: технічного стану кінцевого пристрою, рівня привілеїв користувача та характеристик середовища доступу. Для формування рішення щодо доступу зазначені параметри інтегруються в єдиний показник ризику запиту. У роботі також проведено порівняльний аналіз існуючих підходів до контекстного контролю доступу. Питання забезпечення стійкості КІС в умовах впливу дестабілізуючих чинників досліджено в [10].

Серед сучасних підходів до динамічного оцінювання довіри в роботі Jeong і Yang [11] запропоновано формування інтегральної оцінки на основі адитивного зваженого поєднання чотирьох факторів: поведінки користувача, мережевого середовища, стану пристрою та історії загроз із відповідними ваговими коефіцієнтами 0,4; 0,3; 0,2 та 0,1. У роботі Bradatsch та ін. [12] для оцінювання довіри використано апарат суб’єктивної логіки з урахуванням 29 атрибутів та динамічного порогового значення. Wang та ін. [13] запропоновано поєднання атрибутного контролю доступу (ABAC) з інтегральною оцінкою довіри, для визначення якої використано метод нечіткого аналізу ієрархій (FAHP). У дослідженні Lukaseder та ін. [14] обґрунтовано необхідність урахування контекстних характеристик середовища під час прийняття рішень щодо доступу. У систематичних оглядах архітектури Zero Trust [15], [16] технічний стан пристрою розглядається як один із важливих контекстних факторів оцінювання довіри поряд із поведінкою користувача та його місцезнаходженням. Водночас у зазначених роботах відсутній уніфікований підхід до формування конкретного набору параметрів оцінювання технічного стану кінцевого пристрою.

Проведений аналіз показав, що існуючі дослідження формують теоретичне та методичне підґрунтя для реалізації адаптивного контекстного контролю доступу. Водночас недостатньо дослідженим залишається питання комплексного врахування технічного стану кінцевого пристрою, рівня привілеїв користувача та параметрів середовища доступу під час формування інтегрального показника ризику запиту для КІС

енергетичного сектору. Крім того, потребують подальшого дослідження питання визначення вагових коефіцієнтів контекстних параметрів, порогових значень прийняття рішень щодо доступу та експериментального оцінювання ефективності відповідної моделі.

У попередній роботі авторів [9] сформовано теоретичну основу адаптивної моделі контекстного контролю доступу, числові параметри якої визначаються характеристиками конкретного об'єкта захисту та умовами його функціонування. Тому логічним продовженням проведених досліджень є експериментальна верифікація запропонованої моделі на прикладі КІС енергетичного сектору.

Мета статті – експериментальне дослідження адаптивної моделі контекстного контролю доступу для підвищення стійкості критичних інформаційних систем держави на прикладі енергетичного сектору.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Теоретичною основою дослідження є адаптивна модель контекстного контролю доступу до КІС, запропонована авторами в попередній роботі [9]. Модель передбачає формування множин контекстних параметрів, їх зважену агрегацію в інтегральні показники, визначення інтегрального показника ризику запиту та формування відповідного рішення щодо доступу. У межах цього дослідження здійснюється конкретизація параметрів запропонованої моделі для КІС енергетичного сектору та її подальша експериментальна перевірка.

Контекст запиту доступу до КІС представимо у вигляді кортежу:

$$C = (D, P, CR, WE), \qquad (1)$$

де C – контекст запиту доступу; DP – інтегральний показник технічного стану кінцевого пристрою; CR – коефіцієнт ролі користувача; WE – інтегральний показник середовища доступу.

Для оцінювання технічного стану кінцевого пристрою сформуємо множину відповідних атрибутів:

$$D = \{dp_1, dp_2, \dots, dp_9\}.$$

Інтегральний показник технічного стану кінцевого пристрою визначається шляхом зваженої агрегації нормованих значень відповідних атрибутів:

$$DP = \sum_{i=1}^{9} w_i^{dp} \cdot dp_i, \ \sum_{i=1}^{9} w_i^{dp} = 1, \qquad (2)$$

де $dp_i \in [0; 1]$ – нормоване значення i-го атрибута технічного стану кінцевого пристрою, причому значення 1 відповідає максимальному рівню його захищеності; w_i^{dp} – ваговий коефіцієнт i-го атрибута.

Для врахування рівня привілеїв користувача сформуємо множину ролей $R = \{r_1, r_2, \dots, r_5\}$. Коефіцієнт ролі користувача визначається відображенням $CR: R \to [0, 5, 1, 0]$, при цьому збільшення значення CR відповідає зростанню рівня привілеїв користувача та потенційного впливу компрометації відповідного облікового запису на КІС.

Для оцінювання умов здійснення доступу сформуємо множину атрибутів середовища $\boldsymbol{E} = \{w, e_1, w, e_2 \dots we_{n_{we}}\}$. На основі нормованих значень атрибутів визначається зважена оцінка середовища доступу:

$$E = \sum_{k=1}^{n_{we}} w_k^{we}\, we_k, \ \sum_{k=1}^{n_{we}} w_k^{we} = 1,$$

а інтегральний показник середовища доступу визначається у вигляді:

$$WE = W_{\min} + (W_{\max} - W_{\min})E. \qquad (3)$$

де we_k – нормоване значення k-го атрибута середовища доступу, причому збільшення його значення відповідає зростанню рівня аномальності середовища; w_k^{we} – ваговий коефіцієнт k-го атрибута; $W_{\min}$ та $W_{\max}$ – параметри, що визначають діапазон впливу середовища на інтегральний показник ризику.

На основі отриманих значень DP, CRта WE визначається інтегральний показник ризику запиту доступу:

$$RS = WE \cdot CR \cdot (1 - DP), \qquad (4)$$

де RS – інтегральний показник ризику запиту доступу; $1 - DP$ – залишковий технічний ризик кінцевого пристрою; CR – коефіцієнт, що враховує рівень привілеїв користувача; WE – коефіцієнт, що враховує вплив середовища доступу.

Отримане значення RS використовується для формування рішення щодо доступу. Для цього введемо множину можливих рішень $A = \{A_1, A_2, A_3, A_4\}$, де A_1 – дозвіл на доступ; A_2 – доступ з обмеженнями; A_3 – доступ із додатковою автентифікацією; A_4 – відмова у доступі. Рішення визначається відповідно до порогових значень $\alpha_1 < \alpha_2 < \alpha_3$:

$$\Phi(RS) = \begin{cases} A_1, & RS \le \alpha_1, \\ A_2, & \alpha_1 < RS \le \alpha_2, \\ A_3, & \alpha_2 < RS \le \alpha_3, \\ A_4, & RS > \alpha_3. \end{cases} \qquad (5)$$

Таким чином, для проведення експериментального дослідження необхідно визначити склад множин контекстних параметрів D, R та E, обґрунтувати їх вагові коефіцієнти w_i^{dp}, w_k^{we}, визначити параметри $W_{\min}$, $W_{\max}$та порогові значення α_1, α_2, α_3, а також провести експериментальну перевірку ефективності адаптивної моделі контекстного контролю доступу.

МЕТОДИКА ДОСЛІДЖЕННЯ

Об’єктом дослідження обрано умовну КІС регіонального оператора розподілу електроенергії, що охоплює контур віддаленого та адміністративного доступу до інформаційних систем і засобів віддаленого керування об’єктами АСУ ТП. Вибір такого об’єкта зумовлений актуальністю загроз, пов’язаних із компрометацією віддаленого та підрядного доступу до інформаційно-комунікаційних і технологічних систем енергетичного сектору [6], [8]. Для реалізації адаптивного контекстного контролю доступу розглядається застосування архітектури Zero Trust Network Access (ZTNA), принципи та особливості якої проаналізовано в [15], [16].

Методика проведення експериментального дослідження адаптивної моделі контекстного контролю доступу передбачає виконання п’яти послідовних етапів, загальну схему яких наведено на рис. 1.

Рис. 1. Схема методу експериментального дослідження

На вхід експериментального дослідження надходять множини контекстних параметрів, що характеризують технічний стан кінцевого пристрою, роль користувача та середовище доступу, а також дані щодо сучасних кіберзагроз та інцидентів. У результаті виконання послідовних етапів здійснюється конкретизація параметрів адаптивної моделі, формування експериментальних сценаріїв та оцінювання

ефективності прийняття рішень щодо доступу. Основні параметри експериментального дослідження наведено в табл. 1.

Таблиця 1

Зведені вхідні дані експериментального дослідження

Параметр	Зміст	Значення / діапазон	Спосіб задання
$D = \{dp_1, \ldots, dp_9\}$	множина атрибутів технічного стану кінцевого пристрою	$dp_i \in [0; 1]$	Етап 1
$R = \{r_1, \ldots, r_5\}$	множина ролей користувачів	$CR \in [0, 5, 1, 0]$	Етап 1
$E = we_1, \ldots, we_6$	множина атрибутів середовища доступу	$we_k \in [0; 1]$	Етап 1
w_i^{dp}, w_k^{we}	вагові коефіцієнти атрибутів	$\sum w_i^{dp} = 1;$ $\sum w_k^{we} = 1$	Етап 2
W_{min}, W_{max}	параметри впливу середовища доступу	0,7; 1,6	Етап 2
$\alpha_1, \alpha_2, \alpha_3$	порогові значення прийняття рішень	0,05–0,95; крок 0,05	Етап 5
$S = \{s_1, \ldots, s_N\}$	множина експериментальних сценаріїв запитів доступу	$N = 300$	Етап 4

Етап 1. Формування множин контекстних параметрів

На першому етапі сформуємо множини контекстних параметрів, необхідних для оцінювання запиту доступу до КІС енергетичного сектору. Контекст запиту характеризується технічним станом кінцевого пристрою DP, рівнем привілеїв користувача CR та параметрами середовища доступу WE.

Для визначення інтегрального показника технічного стану кінцевого пристрою DP відповідно до (2) сформовано множину

$$D = \{dp_1, dp_2, \ldots, dp_9\},$$

де dp_1 – актуальність операційної системи та оновлень; dp_2 – стан засобів захисту кінцевих точок (EDR/антивірус); dp_3 – шифрування диска; dp_4 – рівень автентифікації; dp_5 – керованість та відповідність пристрою встановленим вимогам; dp_6 – стан локального міжмережевого екрана; dp_7 – цілісність операційної системи; dp_8 – наявність і чинність сертифіката пристрою; dp_9 – актуальність перевірки технічного стану пристрою.

Доцільність урахування зазначених параметрів зумовлена необхідністю комплексного оцінювання технічного стану кінцевого пристрою під час здійснення доступу до КІС та підтверджується положеннями NIS2 [5], даними щодо сучасних кіберзагроз [6], [7] і результатами досліджень архітектури Zero Trust [15], [16]. Значення атрибутів dp_iнормуються в інтервалі $[0; 1]$, де збільшення значення відповідає підвищенню рівня захищеності кінцевого пристрою.

Для врахування рівня привілеїв користувача та визначення коефіцієнта ролі CR сформовано множину

$$R = \{r_1, r_2, r_3, r_4, r_5\},$$

де r_1 – аудитор; r_2 – оператор; r_3 – диспетчер; r_4 – інженер АСУ ТП; r_5 – адміністратор. Ролі впорядковано відповідно до рівня наданих привілеїв та потенційного впливу компрометації відповідного облікового запису на функціонування КІС.

Для визначення інтегрального показника середовища доступу WE відповідно до (3) сформовано множину:

$$E = \{we_1, we_2, \ldots, we_6\},$$

де we_1 – тип і рівень довіри до мережі доступу; we_2 – географічне місцезнаходження; we_3 – аномалія географічного переміщення користувача; we_4 – часові характеристики запиту; we_5 – репутація IP-адреси; we_6 – поведінкові характеристики користувача. Значення атрибутів we_k нормуються в інтервалі $[0; 1]$, при цьому збільшення значення відповідає зростанню рівня аномальності середовища доступу.

З урахуванням актуальності загроз, пов'язаних із компрометацією ланцюгів постачання та віддаленого доступу до систем енергетичного сектору [8], доступ зовнішнього підрядника враховується під час формування експериментальних сценаріїв як поєднання відповідної ролі користувача, характеристик кінцевого пристрою та параметрів середовища доступу.

Етап 2. Визначення та обґрунтування параметрів адаптивної моделі

На другому етапі визначимо вагові коефіцієнти контекстних параметрів, сформованих на попередньому етапі, та числові значення параметрів адаптивної моделі, необхідні для обчислення DP, CR та WE. Відповідно до базової моделі вагові коефіцієнти можуть визначатися експертним шляхом або на основі статистичного аналізу інцидентів кібербезпеки, що дає змогу адаптувати модель до особливостей конкретної КІС.

Для проведення експериментального дослідження параметри адаптивної моделі визначено таким чином.

1. Вагові коефіцієнти атрибутів технічного стану пристрою w_i^{dp}**.** Значення вагових коефіцієнтів визначено з урахуванням статистичних даних щодо сучасних кіберінцидентів та основних векторів реалізації кіберзагроз [6]–[8]:

$$W^{dp} = \{0{,}14; 0{,}15; 0{,}10; 0{,}12; 0{,}18; 0{,}06; 0{,}13; 0{,}07; 0{,}05\},$$

при цьому $\sum_{i=1}^{9} w_i^{dp} = 1$. Найбільші вагові коефіцієнти встановлено для керованості та відповідності пристрою встановленим вимогам dp_5, стану засобів захисту кінцевих точок dp_2, актуальності операційної системи та оновлень dp_1, а також цілісності операційної системи dp_7.

2. Коефіцієнти ролей користувачів CR**.** Для ролей множини Rвстановлено:

$$CR(r_1) = 0{,}50;\ CR(r_2) = 0{,}65;\ CR(r_3) = 0{,}78;\ CR(r_4) = 0{,}90;\ CR(r_5) = 1{,}00.$$

Збільшення значення CR відповідає зростанню рівня привілеїв користувача та потенційного впливу його дій на функціонування КІС. Така інтерпретація відповідає базовій моделі, у якій ролі користувачів упорядковуються за зростанням їх критичності, а CR використовується як мультиплікативний фактор під час формування інтегрального показника ризику.

3. Вагові коефіцієнти атрибутів середовища доступу w_k^{we}**.** Для атрибутів множини E встановлено:

$$W^{we} = \{0{,}25; 0{,}15; 0{,}20; 0{,}10; 0{,}15; 0{,}15\}$$

,

при цьому $\sum_{k=1}^{6} w_k^{we} = 1$. Найбільші значення вагових коефіцієнтів встановлено для типу та рівня довіри до мережі доступу we_1та аномалії географічного переміщення користувача we_3.

4. Межі зміни інтегрального показника середовища доступу WE**.** У базовій моделі значення $W_{\min}$ та $W_{\max}$визначають межі впливу середовища доступу на інтегральний показник ризику та можуть встановлюватися відповідно до політики безпеки або результатів експертного налаштування. Для проведення експериментального дослідження встановлено:

$$W_{\min} = 0{,}7,\ W_{\max} = 1{,}6.$$

Відповідно до (3) нормована зважена оцінка атрибутів середовища перетворюється до встановленого діапазону, внаслідок чого інтегральний показник середовища доступу змінюється в межах

$$WE \in [0{,}7; 1{,}6],$$

причому збільшення WE відповідає зростанню впливу аномальності середовища на інтегральний показник ризику.

5. Порогові значення прийняття рішень $\alpha_1, \alpha_2, \alpha_3$**.** Порогові значення не задаються апріорно, а визначаються на етапі оцінювання ефективності моделі шляхом калібрування на навчальній вибірці. Такий підхід дає змогу визначити межі переходу між рішеннями A_1–A_4 відповідно до значення інтегрального показника ризику RS. У базовій моделі порогові параметри також розглядаються як параметри політики безпеки або налаштування системи.

Для оцінювання стійкості отриманих результатів до встановлених значень вагових коефіцієнтів на завершальному етапі експериментального дослідження передбачено аналіз чутливості шляхом варіювання w_i^{dp} та w_k^{we} у межах $\pm 20\%$.

Етап 3. Формування еталонної політики прийняття рішень

На третьому етапі сформуємо еталонну політику прийняття рішень щодо доступу для подальшого оцінювання ефективності адаптивної моделі. Еталонні рішення визначаються на основі контекстних параметрів, сформованих на Етапі 1, незалежно від інтегрального показника ризику RS за (4) та порогових значень за (5).

У загальному вигляді еталонну політику представимо як відображення:

$$O_\pi : D \times R \times E \to A, \qquad (6)$$

де O_π – еталонна політика прийняття рішень щодо доступу; D, R, E – множини контекстних параметрів; $A = \{A_1, A_2, A_3, A_4\}$ – множина рішень щодо доступу; π – параметр, що визначає варіант еталонної політики.

Для експериментального дослідження розглянемо два варіанти еталонної політики:

$$\pi \in \{\pi_{sym}, \pi_{dev}\},$$

де π_{sym} передбачає збалансоване врахування технічного стану кінцевого пристрою та параметрів середовища доступу; π_{dev} – пріоритетне врахування технічного стану кінцевого пристрою.

Еталонне рішення $A_1 - A_4$ для кожного сценарію визначається залежно від рівня відхилення контекстних параметрів від штатних значень. Для π_{sym} технічний стан пристрою та параметри середовища враховуються з однаковою пріоритетністю, тоді як для π_{dev} визначальним є технічний стан кінцевого пристрою; рівень привілеїв користувача в обох випадках використовується як додатковий фактор під час формування рішення.

Використання двох варіантів еталонної політики дає змогу оцінити ефективність адаптивної моделі за різної пріоритетності контекстних факторів.

Етап 4. Формування множини експериментальних сценаріїв

На четвертому етапі сформуємо множину експериментальних сценаріїв запитів доступу, необхідних для перевірки адаптивної моделі та її порівняння з іншими підходами до контролю доступу. Для проведення експерименту програмними засобами сформовано множину

$$S = \{s_1, s_2, \ldots, s_N\},\ N = 300,$$

де $s_i = (dp_i, r_i, we_i)$ – окремий сценарій запиту доступу, що характеризується сукупністю значень атрибутів технічного стану кінцевого пристрою, роллю користувача та параметрами середовища доступу.

Формування сценаріїв здійснено на основі чотирьох типових станів кінцевого пристрою: справний керований пристрій, керований пристрій з окремими невідповідностями, некерований особистий пристрій (BYOD) та скомпрометований пристрій у співвідношенні 40 %, 25 %, 20 % та 15 % відповідно. Для середовища доступу визначено корпоративне, віддалене, публічне та потенційно небезпечне середовище у співвідношенні 40 %, 30 %, 20 % та 10 % відповідно. Зазначені співвідношення встановлено для формування експериментальної вибірки, що охоплює як штатні, так і потенційно небезпечні сценарії доступу.

Програмну реалізацію експерименту виконано мовою Python 3.13.3 із використанням бібліотек NumPy 2.5.0 та Matplotlib 3.11.0. Для забезпечення відтворюваності результатів генератор псевдовипадкових чисел ініціалізовано фіксованим значенням $seed = 20260607$.

Для кожного сценарію s_i визначено еталонне рішення відповідно до політик, сформованих на Етапі 3, та рішення запропонованої адаптивної моделі. Для порівняльного оцінювання додатково використано базові підходи RBAC і ABAC, а також моделі контекстного контролю доступу [11], [12].

RBAC реалізовано як статичне прийняття рішення відповідно до ролі користувача, а ABAC – як атрибутну політику, що враховує цілісність, керованість, стан засобів захисту кінцевої точки та актуальність оновлень пристрою.

Для моделі Jeong та Yang [11] використано запропоновану авторами адитивну модель Trust Score, що враховує поведінку користувача B, мережеве середовище N, стан пристрою D та історію загроз T:

$$TS = 0{,}4B + 0{,}3N + 0{,}2D + 0{,}1T. \qquad (7)$$

Оскільки сформована множина Sне містить історичних даних щодо попередніх інцидентів і порушень політик конкретного користувача, значення показника T у межах експерименту прийнято нейтральним.

Підхід Bradatsch et al. [12] використано в адаптованому до сформованої множини експериментальних параметрів вигляді, оскільки Sне містить повного набору атрибутів довіри, необхідних для відтворення оригінального алгоритму. Для експериментального дослідження використано його спрощене представлення на основі доступних контекстних параметрів.

Для забезпечення порівнянності результатів рішення всіх досліджуваних підходів приведено до єдиної множини $A = \{A_1, A_2, A_3, A_4\}$. Для моделей, що формують кількісну оцінку довіри або ризику, порогові значення визначаються за єдиною процедурою на наступному етапі.

Фрагмент результатів програмної реалізації експериментального дослідження наведено на рис. 2.

Вивід симуляційного стенда (experiment_v3.py, Python 3.13.3)

```
$ python experiment_v3.py
======================================================================
v3 (ВИПРАВЛЕНІ ваги Jeong&Yang 0.4/0.3/0.2/0.1) | R=200, seed=20260607

--- ОРАКУЛ 1 (контекст-симетричний): holdout, mean [95% CI] ---
Модель                  Accuracy              macro-F1              FAR
Запропонована           0.596 [0.533;0.653]   0.534 [0.452;0.597]   0.440 [0.333;0.614]
Jeong&Yang              0.677 [0.627;0.733]   0.625 [0.564;0.682]   0.301 [0.200;0.432]
Bradatsch               0.616 [0.560;0.667]   0.528 [0.470;0.579]   0.362 [0.216;0.617]
ABAC                    0.480 [0.427;0.533]   0.366 [0.318;0.411]   0.413 [0.321;0.522]
RBAC                    0.310 [0.260;0.360]   0.118 [0.103;0.132]   1.000 [1.000;1.000]

Стратифікація (accuracy):
  Запропонована            device 0.742 [0.657;0.807]  |  env 0.228 [0.130;0.325]
  Jeong&Yang               device 0.688 [0.620;0.750]  |  env 0.648 [0.537;0.738]

Парна різниця (Запропонована - Jeong&Yang):
  агрегат:      -0.081 [-0.154;-0.007]
  device-страта: 0.054 [-0.048; 0.139]

--- ОРАКУЛ 2 (пристрій-центричний) ---
  Запропонована acc: 0.756 [0.707;0.813]
  Jeong&Yang   acc: 0.380 [0.307;0.440]
  парна різниця (агрегат): 0.376 [0.306;0.454]

OK -> results_v3.json + оновлені fig6/fig7/fig8
```

Рис. 2. Фрагмент результатів програмної реалізації експериментального дослідження

Етап 5. Оцінювання ефективності адаптивної моделі

На п’ятому етапі проведемо оцінювання ефективності адаптивної моделі контекстного контролю доступу на сформованій множині експериментальних сценаріїв S. Оцінювання передбачає калібрування порогових значень, повторне формування навчальної та контрольної вибірок і розрахунок показників якості прийняття рішень.

5.1. Калібрування порогових значень. Для моделей, що формують кількісну оцінку ризику або довіри, порогові значення визначаються на навчальній вибірці шляхом повного перебору можливих комбінацій із множини значень від 0,05 до 0,95 із кроком 0,05:

$$(\alpha_1^*, \alpha_2^*, \alpha_3^*) = F_1^{macro}. \qquad (8)$$

Таким чином, порогові значення не задаються апріорно, а визначаються за результатами калібрування на навчальній вибірці.

5.2. Формування навчальної та контрольної вибірок. Для зменшення залежності результатів від одиничного розбиття множини Sвиконано $Q = 200$ повторних випадкових розбиттів у співвідношенні 50/50 на навчальну та контрольну вибірки. Для кожного розбиття порогові значення визначаються за (8) на навчальній вибірці, після чого показники якості розраховуються на контрольній вибірці. За результатами повторних розбиттів визначаються середні значення показників та 95 % довірчі інтервали.

5.3. Визначення показників якості. Для оцінювання ефективності моделей використано точність класифікації $Accuracy$, макроусереднену F-міру F_1^{macro}, частоту хибного дозволу FAR та частоту хибної відмови FDR. Використання F_1^{macro} додатково до $Accuracy$ зумовлено нерівномірним розподілом еталонних рішень $A_1 - A_4$ у сформованій вибірці. Точність класифікації визначимо як частку рішень моделі, що збігаються з еталонними:

$$Accuracy = \frac{1}{N}\sum_{s=1}^{N} \mathbb{I}\,(\hat{y}_s = y_s), \qquad (9)$$

де $\hat{y}_s$ – рішення моделі для сценарію s; y_s – еталонне рішення; $\mathbb{I}(\cdot)$ – індикаторна функція.

Макроусереднену F-міру визначимо як:

$$F_1^{macro} = \frac{1}{4}\sum_{j=1}^{4} \frac{2P_jR_j}{P_j + R_j}, \qquad (10)$$

де P_j та R_j – точність і повнота для класу рішення A_j.

Для оцінювання помилок, що мають безпосереднє значення для контролю доступу, визначимо частоту хибного дозволу:

$$FAR = \frac{\sum_{s=1}^{N} \mathbb{I}\,(y_s \in \{A_3, A_4\} \wedge \hat{y}_s \in \{A_1, A_2\})}{\sum_{s=1}^{N} \mathbb{I}\,(y_s \in \{A_3, A_4\})}, \qquad (11)$$

та частоту хибної відмови:

$$FDR = \frac{\sum_{s=1}^{N} \mathbb{I}\,(y_s \in \{A_1, A_2\} \wedge \hat{y}_s \in \{A_3, A_4\})}{\sum_{s=1}^{N} \mathbb{I}\,(y_s \in \{A_1, A_2\})}. \qquad (12)$$

Таким чином, на п’ятому етапі визначено процедуру калібрування порогових значень та сукупність показників для оцінювання якості прийняття рішень адаптивною моделлю. Повторне формування навчальної та контрольної вибірок дає змогу отримати усереднені результати та оцінити їх стійкість.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Експериментальне дослідження адаптивної моделі контекстного контролю доступу проведено для умовної КІС регіонального оператора розподілу електроенергії відповідно до розробленої методики.

Для демонстрації процесу формування рішень адаптивною моделлю у табл. 2 наведено результати обчислення показників DP, CR, WE та RS для шести репрезентативних сценаріїв доступу. Порогові значення, отримані в результаті калібрування за критерієм (8), становили: $\alpha_1 = 0{,}10$, $\alpha_2 = 0{,}35$, $\alpha_3 = 0{,}50$.

Таблиця 2

Результати оцінювання репрезентативних сценаріїв доступу

Сценарій	Роль	DP	CR	WE	RS	Рішення	Еталон
Оператор зі справного пристрою, корпоративна мережа	r_2	1,000	0,65	0,700	0,000	A_1	A_1
Адміністратор, керований пристрій, домашня мережа	r_5	1,000	1,00	0,790	0,000	A_1	A_1
Інженер-підрядник, BYOD, публічна мережа	r_4	0,652	0,90	1,127	0,353	A_3	A_3
Диспетчер, аномалія географічного переміщення	r_3	0,964	0,78	1,240	0,035	A_1	A_3
Адміністратор, скомпрометований пристрій, потенційно небезпечне середовище	r_5	0,268	1,00	1,600	1,000	A_4	A_4
Аудитор, домашня мережа	r_1	0,964	0,50	0,835	0,015	A_1	A_1

Розподіл значень інтегрального показника ризику RSза класами еталонних рішень із відповідними каліброваними пороговими значеннями наведено на рис. 3.

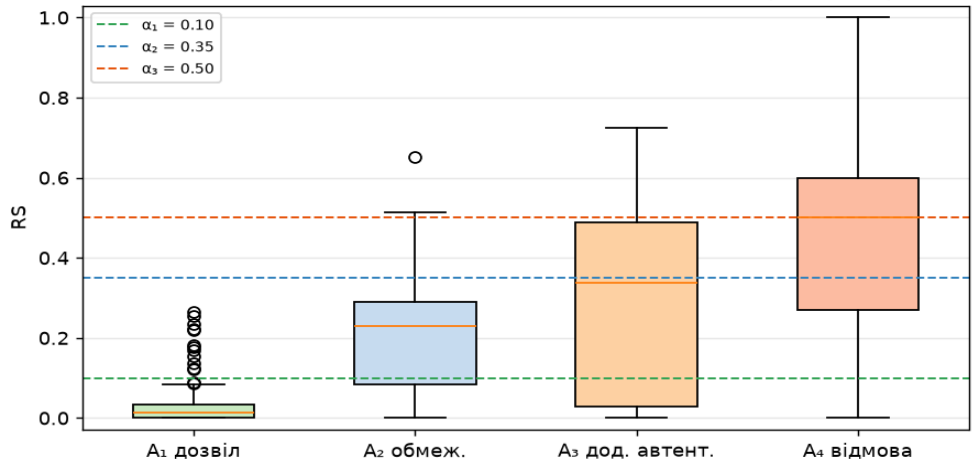

Рис. 3. Розподіл значень RS за класами еталонних рішень та калібровані порогові значення

Результати, наведені в табл. 2, показують відповідність рішень адаптивної моделі еталонним рішенням для п'яти із шести розглянутих сценаріїв. Зокрема, для сценарію доступу інженера-підрядника з BYOD через публічну мережу отримано $RS = 0{,}353$, що відповідає рішенню A_3. Для сценарію доступу адміністратора зі скомпрометованого пристрою в потенційно небезпечному середовищі отримано $RS = 1{,}000$, що відповідає рішенню A_4. В обох випадках рішення адаптивної моделі збігаються з еталонними.

Водночас для сценарію з аномалією географічного переміщення при високому рівні захищеності пристрою ($DP = 0{,}964$) отримано $RS = 0{,}035$, унаслідок чого модель формує рішення A_1 замість еталонного A_3. Такий результат зумовлений мультиплікативною структурою інтегрального показника ризику: при наближенні DP до 1 значення множника $(1 - DP)$ зменшується, що послаблює вплив показника середовища WE на результуюче значення RS.

Порівняльне оцінювання ефективності моделей

Для порівняльного оцінювання ефективності запропонованої адаптивної моделі з підходами Jeong & Yang [11], Bradatsch та ін. [12], ABAC і RBAC використано результати $Q = 200$ повторних розбиттів експериментальної вибірки на навчальну та контрольну частини. Середні значення показників $Accuracy$, F_1^{macro}, FAR і FDR та відповідні 95 % довірчі інтервали для еталонної політики π_{sym} наведено в табл. 3.

Таблиця 3

Результати порівняльного оцінювання моделей за еталонною політикою

Модель	Accuracy	macro-F1	FAR	FDR
Запропонована модель	0,596 [0,533; 0,653]	0,534 [0,452; 0,597]	0,440 [0,333; 0,614]	0,069 [0,021; 0,167]
Jeong & Yang [11]	0,677 [0,627; 0,733]	0,625 [0,564; 0,682]	0,301 [0,200; 0,432]	0,031 [0,000; 0,061]
Bradatsch та ін. [12]	0,616 [0,560; 0,667]	0,528 [0,470; 0,579]	0,362 [0,216; 0,617]	0,079 [0,019; 0,152]
ABAC	0,480 [0,427; 0,533]	0,366 [0,318; 0,411]	0,413 [0,321; 0,522]	0,255 [0,194; 0,313]
RBAC	0,310 [0,260; 0,360]	0,118 [0,103; 0,132]	1,000 [1,000; 1,000]	0,000 [0,000; 0,000]

За результатами порівняльного оцінювання найвище середнє значення $Accuracy$отримано для моделі Jeong & Yang [11] – 0,677, тоді як для запропонованої моделі цей показник становить 0,596. За показником F_1^{macro} модель Jeong & Yang [11] також має найвище значення – 0,625, а запропонована модель – 0,534. Водночас запропонована модель перевищує базові підходи ABAC та RBAC як за $Accuracy$, так і за F_1^{macro}.

Аналіз помилок прийняття рішень показав, що для запропонованої моделі $FAR = 0{,}440$, а $FDR = 0{,}069$. Для RBAC значення $FAR = 1{,}000$, що зумовлено відсутністю врахування контекстних параметрів під час прийняття рішення. Для ABAC характерним є найбільше серед досліджуваних моделей значення $FDR = 0{,}255$, що свідчить про більшу частоту відмов у сценаріях, для яких еталонною політикою передбачено рішення A_1 або A_2.

Графічне представлення середніх значень точності моделей та відповідних 95 % довірчих інтервалів наведено на рис. 4.

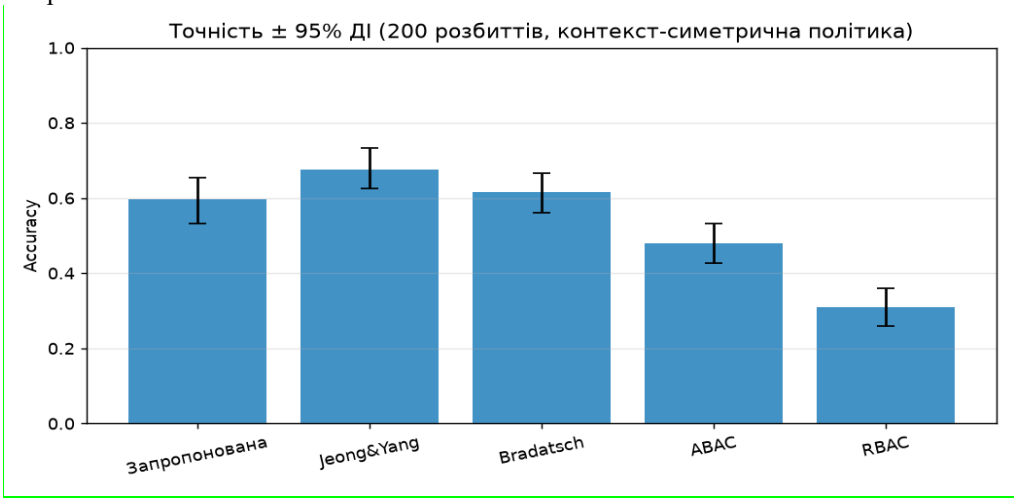

Рис. 4. Точність моделей та 95 % довірчі інтервали за еталонною політикою π_{sym}

Для детальнішого аналізу характеру помилок запропонованої адаптивної моделі на рис. 5 наведено матрицю плутанини, що відображає розподіл сформованих моделлю рішень відносно еталонних класів $A_1 - A_4$.

Рис. 5. Матриця плутанини запропонованої адаптивної моделі

Аналіз ефективності моделей за типами контекстних факторів

Для детальнішого оцінювання ефективності досліджуваних моделей проведено стратифікований аналіз експериментальних сценаріїв залежно від типу контекстних факторів. Окремо розглянуто сценарії, пов'язані з технічним станом кінцевого пристрою, та сценарії, зумовлені аномаліями середовища доступу. Отримані результати наведено в табл. 4.

Таблиця 4

Точність моделей за типами контекстних факторів: середнє значення [95 % ДІ]

Модель	Сценарії, пов'язані з технічним станом пристрою	Сценарії з аномаліями середовища
Запропонована модель	0,742 [0,657; 0,807]	0,228 [0,130; 0,325]
Jeong & Yang [11]	0,688 [0,620; 0,750]	0,648 [0,537; 0,738]
Bradatsch [12]	0,711 [0,632; 0,782]	0,377 [0,256; 0,488]
ABAC	0,605 [0,542; 0,664]	0,165 [0,086; 0,244]
RBAC	0,432 [0,374; 0,500]	0,000 [0,000; 0,000]

Результати стратифікованого аналізу показують, що ефективність моделей істотно залежить від типу контекстних факторів. Для сценаріїв, пов'язаних із технічним станом кінцевого пристрою, запропонована модель демонструє найвище середнє значення точності – 0,742, порівняно з 0,711 для Bradatsch та ін. [12] та 0,688 для Jeong & Yang [11]. Натомість для сценаріїв з аномаліями середовища доступу точність запропонованої моделі становить 0,228, тоді як для Jeong & Yang [11] – 0,648.

Зниження точності запропонованої моделі для сценаріїв з аномаліями середовища пов'язане з мультиплікативною структурою інтегрального показника ризику RS. За високих значень DP множник $(1 - DP)$ наближається до нуля, унаслідок чого вплив WE на результуюче значення RS зменшується. Ця особливість узгоджується з результатом, отриманим раніше для сценарію з аномалією географічного переміщення.

Для статистичного оцінювання відмінностей між запропонованою моделлю та моделлю Jeong & Yang [11] додатково проведено парне порівняння точності на однакових розбиттях експериментальної вибірки. Для всієї вибірки середня парна різниця становить

$$\Delta Accuracy = -0{,}081,\ 95\%\ \text{ДІ} = [-;\, 0{,}154 - 0{,}007].$$

Оскільки довірчий інтервал не містить нульового значення, за еталонної політики π_{sym} різниця є статистично значущою на користь моделі Jeong & Yang [11]. Для сценаріїв, пов'язаних із технічним станом кінцевого пристрою, середня парна різниця становить

$$\Delta Accuracy = +0{,}054,\ 95\%\ \text{ДІ} = [-;\, 0{,}048 + 0{,}139].$$

У цьому випадку довірчий інтервал містить нульове значення, тому статистично значущої різниці між моделями не встановлено, незважаючи на вище середнє значення точності запропонованої моделі.

Результати парного порівняння точності та відповідні 95 % довірчі інтервали наведено на рис. 6.

Вплив еталонної політики на результати оцінювання

Оскільки оцінювання ефективності моделей здійснюється відносно еталонної політики (6), результати порівняння можуть залежати від визначеного значення параметра π. Для оцінювання такого впливу експеримент проведено для двох варіантів еталонної політики: π_{sym}, що передбачає збалансоване врахування технічного стану кінцевого пристрою та параметрів середовища доступу, і π_{dev}, що передбачає пріоритетне врахування технічного стану кінцевого пристрою. Результати порівняння запропонованої моделі та моделі Jeong & Yang [11] наведено в табл. 5.

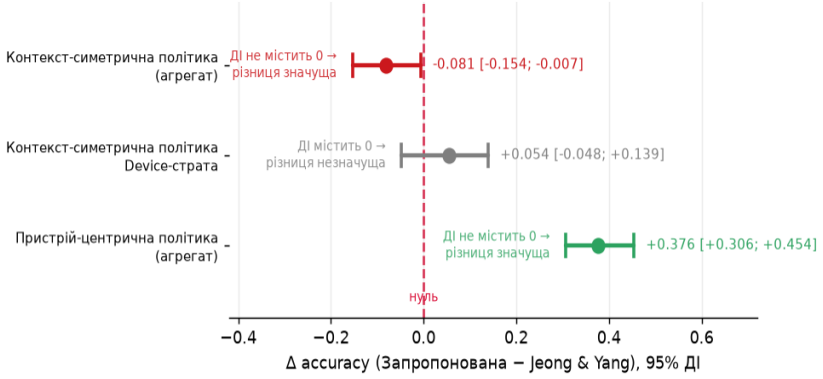

Рис. 6. Парні різниці точності моделей та 95 % довірчі інтервали

Таблиця 5

Вплив еталонної політики на точність досліджуваних моделей

Політика істини	Запропонована модель	Jeong & Yang	Парна різниця
π = sym (контекст-симетрична)	0,596 [0,533; 0,653]	0,677 [0,627; 0,733]	−0,081 [−0,154; −0,007]
π = dev (пристрій-центрична)	0,756 [0,707; 0,813]	0,380 [0,307; 0,440]	+0,376 [+0,306; +0,454]

За еталонної політики π_{sym} середня точність запропонованої моделі становить 0,596, а моделі Jeong & Yang [11] – 0,677. Парна різниця становить −0,081 при 95 % ДІ [−0,154; −0,007], що свідчить про статистично значущу перевагу моделі Jeong & Yang [11] за цього варіанта еталонної політики.

За еталонної політики π_{dev} отримано протилежне співвідношення: точність запропонованої моделі зростає до 0,756, тоді як для моделі Jeong & Yang [11] вона становить 0,380. Парна різниця дорівнює +0,376 при 95 % ДІ [+0,306; +0,454], що свідчить про статистично значущу перевагу запропонованої моделі за пріоритетного врахування технічного стану кінцевого пристрою.

Отримані результати показують, що порівняльна ефективність досліджуваних моделей залежить від пріоритетності контекстних факторів, закладеної в еталонній політиці. Запропонована модель демонструє вищу ефективність за умов пріоритетного врахування технічного стану кінцевого пристрою, тоді як за збалансованого врахування технічного стану пристрою та параметрів середовища вищі результати отримано для адитивної моделі Jeong & Yang [11].

Аналіз чутливості вагових коефіцієнтів

Для оцінювання впливу встановлених вагових коефіцієнтів на результати експериментального дослідження проведено аналіз чутливості шляхом варіювання значень w_i^{dp} та w_k^{we} у межах $\pm 20\%$. Результати показали, що зміна вагових коефіцієнтів у заданих межах не призводить до суттєвих змін точності запропонованої моделі, що свідчить про стійкість отриманих результатів до варіації їх значень.

Результати аналізу чутливості наведено на рис. 7.

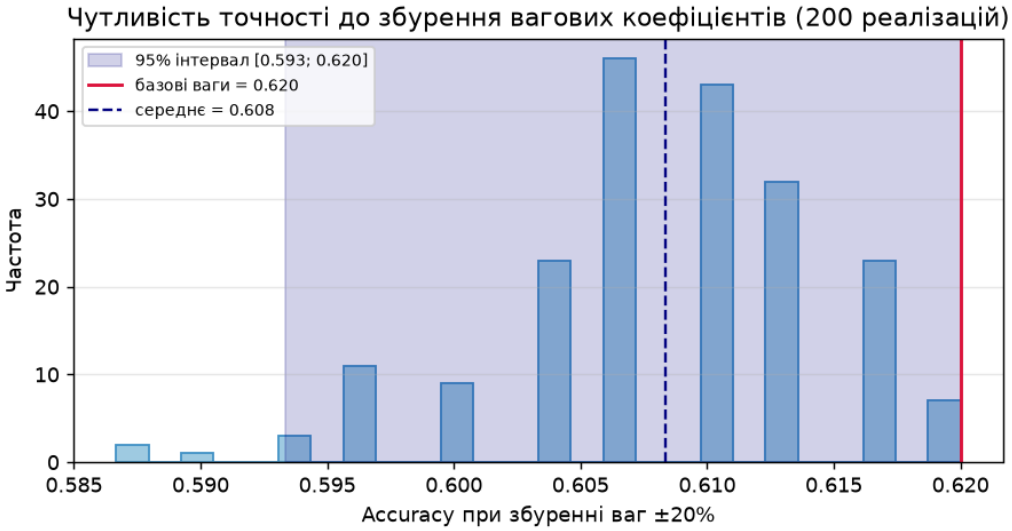

Рис. 7. Чутливість точності запропонованої моделі до зміни вагових коефіцієнтів у межах

Інтерпретація результатів

Отримані результати свідчать про залежність ефективності досліджуваних моделей від способу агрегування контекстних параметрів та їх пріоритетності в еталонній політиці.

По-перше, нижча точність запропонованої моделі для сценаріїв з аномаліями середовища доступу (0,228) пов'язана з мультиплікативною формою (4). При $DP \to 1$значення множника $(1 - DP) \to 0$, унаслідок чого вплив WE на інтегральний показник ризику RS зменшується. Це пояснює зниження чутливості моделі до аномалій середовища за високого рівня захищеності кінцевого пристрою та відповідне значення $FAR = 0{,}440$.

По-друге, адитивна модель Jeong & Yang [11] забезпечує незалежний внесок окремих контекстних факторів у результуючу оцінку, що зумовлює її вищу точність для сценаріїв з аномаліями середовища – 0,648

проти 0,228 для запропонованої моделі. Водночас для сценаріїв, пов'язаних із технічним станом кінцевого пристрою, запропонована модель демонструє вище середнє значення точності – 0,742 проти 0,688 для Jeong & Yang [11].

По-третє, результати порівняння залежать від пріоритетності контекстних факторів, визначеної еталонною політикою (6). За збалансованого врахування технічного стану пристрою та параметрів середовища вищу точність демонструє модель Jeong & Yang [11], тоді як за пріоритетного врахування технічного стану кінцевого пристрою вищу точність має запропонована модель.

Обговорення результатів

Результати експериментального дослідження показали, що запропонована адаптивна модель має переваги у сценаріях, пов'язаних із порушенням технічного стану та компрометацією кінцевих пристроїв. Для цієї групи сценаріїв модель продемонструвала найвище середнє значення точності серед досліджуваних підходів – 0,742. За еталонної політики π_{dev}, що передбачає пріоритетне врахування технічного стану кінцевого пристрою, точність запропонованої моделі становила 0,756 порівняно з 0,380 для моделі Jeong & Yang [11], а парна різниця – +0,376 при 95 % ДІ [+0,306; +0,454].

Водночас за еталонної політики π_{sym} запропонована модель поступається моделі Jeong & Yang [11] за агрегованою точністю, а найбільше зниження ефективності спостерігається для сценаріїв з аномаліями середовища доступу – 0,228 проти 0,648. Виявлена особливість пов'язана з мультиплікативною формою інтегрального показника ризику RS, за якої високий рівень захищеності кінцевого пристрою зменшує вплив параметрів середовища на результуючу оцінку ризику. Аналіз чутливості вагових коефіцієнтів показав, що їх варіювання в межах $\pm 20\%$суттєво не змінює отриманих результатів, що свідчить про структурний характер виявленої особливості.

Отримані результати визначають сферу ефективного застосування запропонованої моделі для КІС, у яких компрометація кінцевого пристрою є одним із пріоритетних факторів ризику. Водночас для систем, у яких аномалії мережевого середовища, географічного розташування або часу доступу мають самостійне критичне значення, доцільним є вдосконалення способу агрегування контекстних параметрів. Перспективним напрямом є поєднання мультиплікативного та адитивного підходів, що дасть змогу зберегти чутливість моделі до стану кінцевого пристрою та водночас посилити врахування аномалій середовища доступу.

Проведене експериментальне дослідження ґрунтується на синтетично сформованій множині сценаріїв для умовної КІС регіонального оператора розподілу електроенергії. Тому наступним етапом дослідження є апробація моделі на реальних даних КІС з розширенням множини сценаріїв доступу.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі проведено експериментальне дослідження адаптивної моделі контекстного контролю доступу для підвищення стійкості критичних інформаційних систем. Для проведення експерименту конкретизовано параметри моделі, сформовано множину сценаріїв доступу та реалізовано програмне оцінювання ефективності запропонованого підходу у порівнянні з відомими моделями контролю доступу.

Отримані результати показали, що ефективність запропонованої моделі залежить від характеру контекстних факторів і профілю загроз КІС. Для сценаріїв, пов'язаних із технічним станом кінцевого пристрою, модель продемонструвала найвище середнє значення точності серед досліджуваних підходів – 0,742. За еталонної політики з пріоритетним урахуванням технічного стану кінцевого пристрою точність запропонованої моделі становила 0,756 порівняно з 0,380 для моделі Jeong & Yang [11]. Водночас установлено необхідність подальшого вдосконалення способу врахування аномалій середовища доступу.

Проведене експериментальне дослідження підтвердило доцільність застосування адаптивної моделі для КІС, у яких технічний стан кінцевого пристрою є одним із пріоритетних факторів ризику, а також необхідність урахування профілю загроз конкретного об'єкта критичної інформаційної інфраструктури під час вибору способу агрегування контекстних параметрів.

Подальші дослідження будуть спрямовані на вдосконалення способу агрегування контекстних параметрів шляхом поєднання мультиплікативного та адитивного підходів, розширення множини експериментальних сценаріїв та апробацію запропонованої моделі на реальних даних КІС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Верховна Рада України. (2021). Про критичну інфраструктуру: Закон України № 1882-IX. https://zakon.rada.gov.ua/laws/show/1882-20

2. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
3. Cybersecurity and Infrastructure Security Agency. (2023). Zero Trust maturity model (Version 2.0). U.S. Department of Homeland Security. https://www.cisa.gov/zero-trust-maturity-model
4. Cloud Security Alliance. (2024). Zero Trust guidance for critical infrastructure. https://cloudsecurityalliance.org/
5. European Parliament and Council. (2022). Directive (EU) 2022/2555 (NIS2). Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
6. European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
7. Verizon. (2025). 2025 data breach investigations report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/
8. Держспецзв'язку, CERT-UA. (2024). Плани UAC-0133 (Sandworm) щодо кібердиверсії на майже 20 об'єктах критичної інфраструктури України [Повідомлення]. https://cert.gov.ua/article/6278706
9. Сидоренко, В. М., & Кобільник, Б. Ю. (2025). Адаптивна модель контекстного контролю доступу для підвищення стійкості критичних інформаційних систем. Кібербезпека: освіта, наука, техніка, 3(31). https://doi.org/10.28925/2663-4023.2025.31.1084
10. Сидоренко, В. М., & Максимець, А. В. (2025). Модель забезпечення стійкості критичних інформаційних систем в умовах впливу внутрішніх та зовнішніх дестабілізуючих чинників. Кібербезпека: освіта, наука, техніка, 3(27). https://doi.org/10.28925/2663-4023.2025.27.779
11. Jeong, E., & Yang, D. (2025). A trust score-based access control model for Zero Trust architecture: Design, sensitivity analysis, and real-world performance evaluation. Applied Sciences, 15(17), 9551. https://doi.org/10.3390/app15179551
12. Bradatsch, L., Miroshkin, O., Trkulja, N., & Kargl, F. (2023). Zero Trust score-based network-level access control in enterprise networks. Proceedings of the 22nd IEEE TrustCom, 1422–1429. https://doi.org/10.1109/TrustCom60117.2023.00194
13. Wang, J., Wang, Z., Song, J., Cheng, H., Cao, Y., & Li, Z. (2023). Attribute and user trust score-based Zero Trust access control model in IoV. Electronics, 12(23), 4825. https://doi.org/10.3390/electronics12234825
14. Lukaseder, T., Halter, M., & Kargl, F. (2020). Context-based access control and trust scores in Zero Trust campus networks. In Sicherheit 2020, LNI (pp. 53–66). Gesellschaft für Informatik. https://doi.org/10.18420/sicherheit2020_04
15. Gambo, M. L., & Almulhem, A. (2025). Zero Trust architecture: A systematic literature review. Journal of Network and Systems Management, 33. https://doi.org/10.1007/s10922-025-09998-x
16. Zohaib, S. M., Sajjad, S. M., Iqbal, Z., Yousaf, M., Haseeb, M., & Muhammad, Z. (2024). Zero Trust VPN (ZT-VPN): A systematic literature review and cybersecurity framework for hybrid and remote work. Information, 15(11), 734. https://doi.org/10.3390/info15110734

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Viktoriia Sydorenko
PhD, Associate Professor, Department of Computer Information Technologies
National University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Bohdan Kobilnyk
PhD Student, Faculty of Computer Science and Technology
National University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID: 0009-0001-4848-541X
2539821@stud.kai.edu.ua

EXPERIMENTAL STUDY OF AN ADAPTIVE CONTEXTUAL ACCESS CONTROL MODEL FOR ENHANCING THE RESILIENCE OF CRITICAL INFORMATION SYSTEMS

Abstract. In the context of the growing number and increasing complexity of cyber threats, ensuring secure access to critical information systems (CIS) is one of the key tasks in protecting the state's critical information infrastructure. The use of adaptive access control mechanisms capable of accounting for changes in endpoint device posture, user privilege levels, and access environment parameters in accordance with the principles of the Zero Trust architecture is becoming increasingly important. This article presents an experimental study of an adaptive contextual access control model aimed at enhancing the resilience of CIS. To conduct the experiment, the model parameters were specified taking into account the characteristics of energy-sector CIS, a set of access scenarios was formed, and a software-based evaluation of the proposed approach was performed in comparison with existing access control models. The experimental results confirmed the adequacy and operability of the proposed model, as well as its ability to adaptively make access decisions in response to changes in contextual parameters. For scenarios related to endpoint device posture, the model demonstrated the highest average accuracy among the approaches considered, reaching 0.742, while under the reference policy prioritizing endpoint device posture, its accuracy reached 0.756. The results confirmed the feasibility of applying the proposed model to CIS in which endpoint device posture is one of the priority risk factors. The practical significance of the obtained results lies in the possibility of applying the developed model to build adaptive contextual access control systems for CIS while taking into account the threat profile of a specific critical information infrastructure facility. Further research will focus on improving the method for aggregating contextual parameters, expanding the set of experimental scenarios, and validating the proposed model using real-world CIS data.

Keywords: critical information systems; critical infrastructure; contextual access control; adaptive model; Zero Trust; risk assessment; cybersecurity; resilience.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Verkhovna Rada of Ukraine. (2021). On critical infrastructure: Law of Ukraine No. 1882-IX. https://zakon.rada.gov.ua/laws/show/1882-20
2. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust architecture (NIST SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
3. Cybersecurity and Infrastructure Security Agency. (2023). Zero Trust maturity model (Version 2.0). U.S. Department of Homeland Security. https://www.cisa.gov/zero-trust-maturity-model
4. Cloud Security Alliance. (2024). Zero Trust guidance for critical infrastructure. https://cloudsecurityalliance.org/
5. European Parliament and Council. (2022). Directive (EU) 2022/2555 (NIS2). Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

6. European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
7. Verizon. (2025). 2025 data breach investigations report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/
8. Computer Emergency Response Team of Ukraine. (2024). UAC-0133 (Sandworm) plans for cyber sabotage at almost 20 critical infrastructure facilities in Ukraine [Advisory]. CERT-UA. https://cert.gov.ua/article/6278706
9. Sydorenko, V. M., & Kobilnyk, B. Yu. (2025). Adaptive contextual access control model for enhancing the resilience of critical information systems. Cybersecurity: Education, Science, Technique, 3(31). https://doi.org/10.28925/2663-4023.2025.31.1084
10. Sydorenko, V. M., & Maksymets, A. V. (2025). Model for ensuring the resilience of critical information systems under the influence of internal and external destabilizing factors. Cybersecurity: Education, Science, Technique, 3(27). https://doi.org/10.28925/2663-4023.2025.27.779
11. Jeong, E., & Yang, D. (2025). A trust score-based access control model for Zero Trust architecture: Design, sensitivity analysis, and real-world performance evaluation. Applied Sciences, 15(17), 9551. https://doi.org/10.3390/app15179551
12. Bradatsch, L., Miroshkin, O., Trkulja, N., & Kargl, F. (2023). Zero Trust score-based network-level access control in enterprise networks. Proceedings of the 22nd IEEE TrustCom, 1422–1429. https://doi.org/10.1109/TrustCom60117.2023.00194
13. Wang, J., Wang, Z., Song, J., Cheng, H., Cao, Y., & Li, Z. (2023). Attribute and user trust score-based Zero Trust access control model in IoV. Electronics, 12(23), 4825. https://doi.org/10.3390/electronics12234825
14. Lukaseder, T., Halter, M., & Kargl, F. (2020). Context-based access control and trust scores in Zero Trust campus networks. In Sicherheit 2020, LNI (pp. 53–66). Gesellschaft für Informatik. https://doi.org/10.18420/sicherheit2020_04
15. Gambo, M. L., & Almulhem, A. (2025). Zero Trust architecture: A systematic literature review. Journal of Network and Systems Management, 33. https://doi.org/10.1007/s10922-025-09998-x
16. Zohaib, S. M., Sajjad, S. M., Iqbal, Z., Yousaf, M., Haseeb, M., & Muhammad, Z. (2024). Zero Trust VPN (ZT-VPN): A systematic literature review and cybersecurity framework for hybrid and remote work. Information, 15(11), 734. https://doi.org/10.3390/info15110734

Отримано редакцією журналу / Received: 20.02.26
Прорецензовано / Revised: 28.02.26
Схвалено до друку / Accepted: 24.09.26