КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1084
УДК 004.056.5:004.7

Сидоренко Вікторія Миколаївна
к.т.н., доцент, доцент кафедри комп'ютерних інформаційних технологій
Державний 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
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0009-0001-4848-541X
2539821@stud.kai.edu.ua

АДАПТИВНА МОДЕЛЬ КОНТЕКСТНОГО КОНТРОЛЮ ДОСТУПУ ДЛЯ ПІДВИЩЕННЯ СТІЙКОСТІ КРИТИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація. В роботі запропоновано модель адаптивного контролю доступу для критичних інформаційних систем, що інтегрує три групи атрибутів: технічний стан пристрою (Device Posture), роль користувача та параметри середовища доступу. На основі аналізу сучасних підходів Zero Trust обґрунтовано необхідність багатофакторного оцінювання ризику під час кожного запиту доступу. Розроблена модель формує інтегральний показник ризику на основі вагових коефіцієнтів та контекстних параметрів, забезпечуючи динамічне ухвалення рішень у вигляді дозволу, обмеженого доступу, додаткової автентифікації або відмови. Запропонований підхід підвищує точність виявлення ризикових сценаріїв та сприяє зміцненню стійкості критичних інформаційних систем. Перспективи подальших досліджень передбачають розширення моделі за рахунок поведінкових атрибутів, використання статистичних даних, застосування методів машинного навчання для адаптивного коригування вагових коефіцієнтів і порогових значень, а також проведення експериментальної валідації запропонованої моделі.

Ключові слова: критичні інформаційні системи, оцінка ризику, Zero Trust, контроль доступу, контекстний контроль, адаптивні політики доступу, Device Posture, стійкість, кібербезпека.

ВСТУП

Сучасні критичні інформаційні системи (КІС) [1] функціонують у середовищі, що характеризується високою динамічністю, розподіленістю цифрових сервісів, широким застосуванням хмарних інфраструктур і мобільністю користувачів. Такі умови формують новий ландшафт ризиків, у якому традиційні периметрові моделі безпеки поступово втрачають ефективність. Поширення тактик латерального руху, а також можливість швидкого поширення компрометації з однієї кінцевої точки на всю систему зумовлюють потребу у відмові від презумпції довіри до внутрішнього сегменту мережі.

Архітектура Zero Trust, концептуально окреслена у NIST SP 800-207, пропонує принципово нову парадигму: «ніколи не довіряй, завжди перевіряй» [2]. У Zero Trust Network Access (ZTNA) рішення про доступ ґрунтується не на розташуванні користувача в мережі, а на оцінюванні кожного окремого запиту з урахуванням стану пристрою, поведінкових характеристик суб'єкта та контексту середовища. Це перетворює контроль доступу на динамічний процес, який має бути чутливим до змін ризикового профілю у реальному часі.

Попри поширеність традиційних механізмів контролю доступу – Role-Based Access Control (RBAC) та Attribute-Based Access Control (ABAC) – їхня статичність створює суттєві обмеження в умовах динамічних загроз. RBAC забезпечує впорядкованість політик, але не враховує зміни стану пристрою та поведінки користувача під час сесії [3]. ABAC забезпечує більшу гнучкість, однак у базовій формі не включає механізму безперервної оцінки довіри чи ризику [4]. У результаті навіть формально коректний запит може бути небезпечним, якщо, наприклад, пристрій користувача немає актуальних оновлень, працює без шифрування диску або демонструє ознаки компрометації.

У сучасних дослідженнях Zero Trust дедалі більше уваги приділяється підходам, що інтегрують кількісні моделі оцінювання ризику, зокрема trust-score, у процес ухвалення рішень. Проте наявні рішення часто зосереджені переважно на поведінкових або мережевих атрибутах, залишаючи поза увагою формалізовану оцінку технічного стану пристрою (Device Posture), рівня привілеїв користувача або зовнішніх умов доступу. Така неповнота призводить до того, що існуючі моделі лише частково відповідають вимогам ZTNA у контексті забезпечення стійкості КІС.

Постановка проблеми. У КІС контроль доступу традиційно ґрунтується на статичних правилах, що визначають набір прав користувача та межі його взаємодії з ресурсами системи. У випадку застосування RBAC або ABAC рішення про доступ базується на попередньо визначених характеристиках суб’єкта або об’єкта, тоді як поточний стан середовища та пристрою не враховується. Такий підхід є недостатнім в умовах зростання кількості інцидентів, пов’язаних із компрометацією користувацьких пристроїв, використанням вразливостей кінцевих точок та зловживанням привілеями.

Впровадження принципів Zero Trust потребує переходу від фіксованих авторизаційних правил до динамічного контролю, де кожен запит доступу оцінюється з урахуванням актуального ризику. Це вимагає аналізу технічного стану пристрою, рівня привілеїв користувача та параметрів середовища в момент звернення. Відсутність формалізованого механізму інтеграції цих факторів у єдину процедуру прийняття рішення обмежує можливості КІС щодо запобігання несанкціонованому доступу та реагування на загрози, що швидко змінюються.

Таким чином, виникає необхідність у створенні нової моделі контролю доступу, здатної динамічно враховувати контекст взаємодії та забезпечувати адаптивне коригування прав відповідно до рівня ризику. Така модель повинна забезпечувати оцінювання Device Posture, вплив рівня привілеїв користувача та умов середовища у поєднанні з можливістю ухвалення рішень у реальному часі. Її застосування сприятиме посиленню стійкості КІС у процесі протидії сучасним кіберзагрозам. Саме така модель є критичною для підвищення кіберстійкості КІС в умовах постійно еволюціонуючих загроз.

Аналіз останніх досліджень і публікацій. У наукових дослідженнях, присвячених удосконаленню контролю доступу в умовах Zero Trust, спостерігається активний розвиток підходів, що інтегрують динамічну оцінку ризику у процес ухвалення рішень. Одним із ключових напрямів є використання trust-score – узагальненої кількісної оцінки довіри, сформованої на основі поведінкових, технічних та контекстних атрибутів.

У роботі Jeong & Yang (2025) [5] запропоновано модель, у якій рішення про доступ ґрунтується на інтегрованому trust-score, отриманому шляхом аналізу поведінкових та контекстних сигналів. Модель демонструє переваги переходу до динамічної авторизації, однак технічний стан пристрою розглядається лише частково, без виокремлення його як самостійної метрики.

У дослідженні Bradatsch et al. (2023) [6] застосовано підхід на основі суб’єктивної логіки, що включає 29 атрибутів для побудови trust-score. Автори зосереджуються

переважно на мережевих характеристиках і поведінці, тоді як стан кінцевого пристрою, рівень привілеїв користувача та їхній взаємозв'язок у контексті ризику не формалізовані.

Модель Wang et al. (2023) [7] інтегрує елементи ABAC з trust-score, обчисленим методом FAHP. Підхід забезпечує гнучкість і часткову адаптивність, однак використовує trust-score переважно як поведінкову метрику. Device Posture та роль користувача в моделі не розглядаються як окремі фактори, що знижує застосовність підходу в КІС, де компрометація кінцевих точок та зловживання привілеями мають критичні наслідки.

У роботі Lukaseder et al. (2020) [8] підкреслено важливість контекстних характеристик – часу, місця та типу підключення. Автори демонструють роль середовища в адаптивному контролі доступу, проте відсутній механізм поєднання контексту з технічним станом пристрою та ієрархією користувацьких прав.

Додатково варто врахувати положення, викладені у документі (CISA, 2023) [9]. У моделі підкреслюється, що Zero Trust ґрунтується на принципах постійної перевірки, мінімальної довіри та адаптивного управління доступом, що передбачає динамічне оцінювання контексту кожної взаємодії. CISA наголошує на необхідності врахування технічного стану пристрою, поведінкових сигналів та параметрів середовища доступу, оскільки статичні механізми авторизації не забезпечують достатнього рівня захисту у сучасних умовах. Такий підхід узгоджується з результатами досліджень [8] et al. (2020) і підтверджує доцільність використання багатофакторних адаптивних моделей контролю, здатних реагувати на зміну ризиків під час сесії доступу.

Окрім trust-score підходів, у наукових джерелах представлена ціла низка досліджень, присвячених контекстуальним моделям доступу. У Singh (2025) [11] запропоновано метрик-орієнтовану модель контекстного контролю доступу в хмарних середовищах. Автор акцентує на важливості багатофакторного аналізу, однак модель не формалізує оцінку Device Posture і не містить кількісного ризик-скорингу, який підходив би для ZTNA.

У роботі Herrera et al. (2022) [12] розглядається контекстуальна авторизація з акцентом на приватність. Незважаючи на високий рівень деталізації контекстних змінних, модель не включає технічний стан пристрою як ключовий показник надійності доступу.

У табл. 1, систематизовано та представлено детальний аналіз підходів до контролю доступу в архітектурі Zero Trust описаних у проаналізованих джерелах за такими 7 критеріями (запропоновані авторами):

1. Інтегрований показник ризику (RS) – наявність єдиного числового показника довіри або ризику, що формується на основі сукупності атрибутів доступу та використовується для прийняття рішень авторизації.
2. Стан кінцевого пристрою (DP) – урахування технічного та безпекового стану пристрою користувача (оновлення, конфігурація, відповідність політикам) під час контролю доступу.
3. Поведінкові атрибути (BA) – використання характеристик поведінки користувача (патерни активності, аномалії, історія доступу) для оцінювання рівня довіри.
4. Контекст доступу (CTX) – урахування зовнішніх умов доступу, зокрема часу, геолокації, типу мережі та середовища підключення.
5. Рівень привілеїв (PRIV) – диференціація ризиків і політик доступу залежно від ролі та рівня привілеїв користувача.
6. Адаптивність під час сесії (ADP) – здатність системи динамічно змінювати або обмежувати доступ у межах активної сесії при зміні ризикових факторів.
7. Придатність до КІС (CIS) – відповідність підходу вимогам безпеки, стійкості та контролю доступу в КІС.

Таблиця 1

Порівняльний аналіз підходів контролю доступу в архітектурі Zero Trust

№	Назва	Критерії						
		RS	**DP**	**BA**	**CTX**	**PRIV**	**ADP**	**CIS**
1.	Jeong & Yang	+	+/-	+	+	-	+	+/-
2.	Bradatsch et al.	+	-	+	+/-	-	+/-	+/-
3.	Wang et al.	+	-	+	+/-	+/-	+/-	+/-
4.	Lukaseder et al.	+/-	-	+/-	+	-	+	+/-
5.	Singh	-	-	-	+	-	+/-	-
6.	Herrera et al.	-	-	-	+	-	+/-	-

Значний внесок у формування теоретичного підґрунтя для моделей стійкості та ризик-орієнтованого контролю внесено Сидоренко & Максимцем (2025) [10]. Автори пропонують системний підхід до оцінювання стійкості КІС, у якому аналізуються внутрішні та зовнішні дестабілізуючі чинники. У моделі формалізовано підходи до інтегральної оцінки стану системи, проте вона не є моделлю контролю доступу і не враховує специфіки авторизаційних рішень у контексті Zero Trust. Водночас концептуальна рамка роботи підкреслює важливість багатофакторного оцінювання та адаптивності – властивостей, які є ключовими для розроблення сучасних моделей ZTNA.

Актуальними для дослідження є також підходи, описані в Avtushenko et al. (2022) [13], де розглянуто механізми оцінювання захищеності інформаційних систем та принципи раціональної побудови комплексних моделей. Хоча робота не торкається Zero Trust безпосередньо, вона формує методологічне підґрунтя для побудови структурованих систем оцінки.

Таким чином, узагальнення літератури дозволяє окреслити спільні обмеження сучасних моделей:

1. Відсутність структурованого обліку Device Posture як критичного фактору ризику;
2. Відсутність ризикової диференціації відповідно до рівня привілеїв користувача;
3. Обмежена інтеграція атрибутів середовища у формальний числовий показник;
4. Відсутність цілісної формальної функції ризик-скорингу, придатної для реального часу;
5. Відсутність оркестраційної логіки, яка може керувати адаптивними політиками доступу.

Таким чином, є необхідність розроблення моделі, що об’єднує технічні, поведінкові та контекстні атрибути у єдиний механізм адаптивного контролю доступу, відповідний вимогам Zero Trust у КІС.

Метою статті є розроблення адаптивної моделі контекстного контролю доступу для підвищення стійкості КІС держави.

ТЕОРЕТИЧНІ ОСНОВИ РОЗРОБКИ МОДЕЛІ

Побудова моделі адаптивного контекстного контролю доступу в КІС

Модель передбачає формування декількох груп атрибутів, що відображають технічний стан пристрою (Device Posture), рівень привілеїв користувача та параметри середовища доступу. Для інтеграції цих факторів необхідно визначити спосіб їх нормування, вагові коефіцієнти та механізм впливу на інтегральну оцінку ризику.

Побудова моделі охоплює такі ключові положення:

1. Кожен атрибут має бути кількісно вимірюваним;
2. Ваги атрибутів повинні відображати їх відносну критичність;
3. Функція ризику має бути чутливою до зниження рівня безпеки будь-якої з груп атрибутів;
4. Отримана оцінка повинна відповідати принципам Zero Trust, де кожен запит перевіряється незалежно від попередніх.

Етап 1. Формалізація атрибутів контексту та їх оцінювання

У межах моделі адаптивного контекстного контролю доступу формуються три групи атрибутів, що комплексно характеризують ризиковий стан запиту доступу. Застосування цих атрибутів відповідає підходам, запропонованим у роботах Jeong & Yang (2025) [5], Wang et al. (2023) [7] та Lukaseder et al. (2020) [8], де наголошується на важливості поєднання технічних, поведінкових і контекстних факторів у Zero Trust.

Контекст доступу до КІС формалізується у вигляді сукупності контекстних атрибутів:

$$C = (DP, CR, WE), \tag{1}$$

де DP – інтегральний показник технічного стану пристрою, CR – коефіцієнт ролі користувача, WE – інтегральний показник середовища доступу.

Крок 1.1. Формалізація технічного стану пристрою

Множина атрибутів технічного стану пристрою визначається як:

$$DP = \left\{ dp_1, dp_2, ..., dp_{n_{dp}} \right\}, \tag{2}$$

де $dp_i \in [0;1]$ – нормований параметр технічного стану пристрою, n_{dp} – кількість атрибутів технічного стану.

Інтегральний показник технічного стану пристрою визначається зваженою агрегацією:

$$DP = \sum_{i=1}^{n_{dp}} w_i^{dp} \cdot dp_i, \ \sum_{i=1}^{n_{dp}} w_i^{dp} = 1, \tag{3}$$

де w_i^{dp} – ваговий коефіцієнт i-го атрибуту технічного стану пристрою.

Крок 1.2. Формалізація коефіцієнта ролі користувача

Введемо множину ролей користувачів у системі, у наступному вигляді:

$$R = \left\{ r_1, r_2, ..., r_{n_r} \right\}, \tag{4}$$

де $r_j \in [0;1]$ – множина ролей користувачів у системі, n_r – кількість ролей користувачів.

Коефіцієнт ролі користувача визначається як:

$$CR = CR(r_j), r_j \in R, \tag{5}$$

де $CR(r_j)$ – значення коефіцієнта ролі, що відповідає ролі користувача r_j.

Крок 1.3. Формалізація атрибутів середовища доступу

Множина атрибутів середовища доступу визначається як:

$$WE = \left\{ we_1, we_2, ..., we_{n_{we}} \right\}, \tag{6}$$

де $we_k \in [0;1]$ – нормований параметр середовища доступу, n_{we} – кількість атрибутів середовища.

Інтегральний показник середовища доступу визначається у вигляді:

$$WE = \sum_{k=1}^{n_{we}} w_k^{we} \cdot we_k, \ \sum_{k=1}^{n_{we}} w_k^{we} = 1, \quad (7)$$

де w_k^{we} – ваговий коефіцієнт k-го атрибуту середовища доступу.

Етап 2. Формальне оцінювання технічного стану пристрою (Device Posture, DP)

Оцінювання технічного стану кінцевого пристрою здійснюється на основі множини атрибутів DP, введеної за допомогою (2).

Кожен атрибут технічного стану нормується у діапазоні:

$$dp_i \in [0;1], \quad (8)$$

де dp_i – i-й параметр технічного стану пристрою; $dp_i = 0$ – відповідає критично небезпечному або неприйнятному стану, $dp_i = 1$ – максимально допустимому рівню захищеності.

Інтегральний показник технічного стану пристрою визначається шляхом лінійної зваженої агрегації нормованих атрибутів:

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

де w_i – ваговий коефіцієнт i-го атрибуту технічного стану, n_{dp} – кількість атрибутів технічного стану.

Вагові коефіцієнти задовольняють умову нормування:

$$\sum_{i=1}^{n_{dp}} w_i = 1. \quad (10)$$

Значення вагових коефіцієнтів можуть визначатися експертним шляхом або на основі статистичного аналізу інцидентів інформаційної безпеки, що дозволяє адаптувати модель до особливостей конкретної КІС.

Отримане значення DP є кількісною оцінкою технічного стану кінцевого пристрою та використовується на наступних етапах моделі для формування інтегральної оцінки ризику запиту доступу.

Для формалізованої інтерпретації значень показника DP вводиться множина рівнів технічного стану пристрою:

$$L_{DP} = \{L_0, L_1, L_2, L_3\} \quad (11)$$

де L_j – j-й формальний рівень технічного стану кінцевого пристрою.

Таблиця 2

Формальне розбиття інтегрального показника технічного стану пристрою

Інтервал значення DP	Рівень технічного стану
$DP \in [0; Q_1)$	L_0
$DP \in [Q_1; Q_2)$	L_1
$DP \in [Q_2; Q_3)$	L_2
$DP \in [Q_3; 1]$	L_3

де $Q_1, Q_2, Q_3 \in (0;1)$ – порогові параметри класифікації інтегрального показника технічного стану пристрою, $Q_1 < Q_2 < Q_3$.

Етап 3. Формальне оцінювання коефіцієнта ролі користувача (CR)

Коефіцієнт ролі користувача CR визначається відповідно до (4) та використовується для врахування впливу рівня привілеїв користувача на інтегральний ризик доступу.

Для формалізованої інтерпретації значень коефіцієнта ролі вводиться множина рівнів ролей користувачів:

$$L_{CR} = \left\{ L_1^{CR}, L_2^{CR}, ..., L_k^{CR} \right\}, \tag{12}$$

де L_j^{CR} – формальний рівень ролі користувача, що відповідає зростанню рівня привілеїв, а k – кількість ролей користувачів у системі.

Відповідність між ролями користувачів та рівнями L_{CR} задається відношенням впорядкування:

$$r_1 \prec r_2 \prec ... \prec r_k, \tag{13}$$

де символ $\prec$ означає зростання критичності ролі користувача.

Отримане значення коефіцієнта CR використовується на наступних етапах моделі як мультиплікативний фактор ризику під час формування інтегральної оцінки ризику запиту доступу.

Етап 4. Інтерпретація та використання показника середовища доступу (WE)

Атрибути середовища доступу (Working Environment, WE) відображають зовнішні умови, у яких користувач взаємодіє з КІС, та виконують коригувальну функцію під час оцінювання ризику запиту доступу. На відміну від технічного стану пристрою та рівня привілеїв користувача, параметри середовища мають динамічний характер і можуть змінюватися залежно від типу мережі, геолокації, часових характеристик і поведінкових відхилень.

Формування множини атрибутів середовища доступу WE, їх нормування та агрегування в інтегральний показник WE здійснюється відповідно до (7)–(8). Отримане значення WE використовується в подальшому як коригувальний коефіцієнт, що підсилює або послаблює вплив інших складових моделі ризику залежно від контексту запиту.

Область значень показника WE

Інтегральний показник середовища доступу належить обмеженому інтервалу:

$$WE \in \left[W_{\min}, W_{\max} \right], \tag{14}$$

де $W_{\min} < 1$ – відповідає умовам зниженого контекстного ризику, $WE = 1$ – відповідає нейтральному середовищному контексту, що не змінює інтегральну оцінку ризику, $W_{\max} > 1$ – відповідає умовам підвищеного контекстного ризику.

Значення $WE = 1$ відповідає нейтральному середовищному контексту та не змінює інтегральну оцінку ризику запиту доступу.

Значення параметрів $W_{\min}$ та $W_{\max}$ визначаються політиками безпеки організації або результатами експертного налаштування і не фіксуються у межах формального опису методу.

Формальна класифікація станів середовища доступу

Для уніфікованої інтерпретації значень показника *WE* вводиться множина рівнів середовища доступу:

$$L_{WE} = \left\{ L_1^{WE}, L_2^{WE}, ..., L_q^{WE} \right\}, \tag{15}$$

де L_i^{WE} – формальний рівень середовищного контексту, що відповідає зростанню контекстного ризику.

Віднесення значення *WE* до відповідного рівня здійснюється за пороговими параметрами:

$$W_1 > W_2 > ... > W_q, \tag{16}$$

де $W_i \in [W_{\min}, W_{\max}]$.

Роль показника WE у загальній моделі ризику

Показник *WE* не є самостійним джерелом ризику, а виконує функцію контекстного коригування, забезпечуючи адаптивність моделі відповідно до принципів **continuous evaluation**, характерних для архітектур Zero Trust. На наступних етапах *WE* інтегрується з показником технічного стану пристрою *DP* та коефіцієнтом ролі користувача *CR* для формування інтегральної оцінки ризику запиту доступу до КІС.

Етап 5. Формування інтегрального показника ризику (Risk Score, RS)

Після формалізації показників технічного стану пристрою *DP*, коефіцієнта ролі користувача *CR* та середовища доступу *WE* здійснюється їх інтеграція в єдиний кількісний показник ризику запиту доступу до КІС відповідно до принципів Zero Trust [2].

Інтегральний показник ризику визначається як функція:

$$RS = f(DP, CR, WE). \tag{17}$$

З урахуванням ролі показника середовища доступу як коригувального коефіцієнта, а також інтерпретації величини $1 - DP$ як залишкового технічного ризику кінцевого пристрою, функцію (17) конкретизовано у вигляді мультиплікативної моделі:

$$RS = WE \cdot CR \cdot (1 - DP), \tag{18}$$

де $1 - DP$ – залишковий технічний ризик кінцевого пристрою; *CR* – коефіцієнт, що враховує рівень привілеїв користувача; *WE* – коригувальний коефіцієнт середовища доступу.

Запропонована форма забезпечує чутливість інтегрального показника до змін кожної зі складових та враховує підсилювальний ефект їх поєднання, що відповідає сучасним ризик-орієнтованим моделям контролю доступу [6].

Отримане значення *RS* використовується на наступному етапі методу для ухвалення рішення щодо доступу до КІС.

Етап 6. Формалізована модель ухвалення рішення про доступ

На основі інтегрального показника ризику *RS*, сформованого відповідно до Етапу 5, здійснюється ухвалення рішення щодо надання доступу до КІС. Рішення про доступ ґрунтується на поточній оцінці ризику контексту запиту відповідно до принципів Zero Trust [2].

Формалізація множини рішень доступу

Введемо множину можливих рішень щодо доступу:

$$A = \left\{ A_1, A_2, A_3, A_4 \right\}, \tag{19}$$

де A_1 – дозвіл на доступ, A_2 – доступ з обмеженнями, A_3 – доступ із додатковою автентифікацією, A_4 – відмова у доступі.

Порогова інтерпретація інтегрального ризику

Інтегральний показник ризику належить інтервалу:

$$RS \in [0;1], \tag{20}$$

Для інтерпретації значень RS вводиться множина порогових параметрів:

$$0 < \tau_1 < \tau_2 < \tau_3 < 1, \tag{21}$$

які визначають межі між рівнями ризику та задаються політиками безпеки або параметрами налаштування системи.

Процедура ухвалення рішення формалізується у вигляді відображення:

$$\Phi : RS \to A, \tag{22}$$

яке визначається співвідношенням:

$$\Phi(RS) = \begin{cases} A_1, RS \le \tau_1, \\ A_2, \tau_1 < RS \le \tau_2, \\ A_3, \tau_2 < RS \le \tau_3, \\ A_4, RS > \tau_3. \end{cases} \tag{23}$$

Таблиця 3

Формалізована модель ухвалення рішення про доступ на основі інтегрального показника ризику

Інтервал значень RS	**Формальне рішення A_i**	**Тип доступу**	**Характеристика рішення**
$RS \le \tau_1$	A_1	Дозвіл на доступ	Доступ без додаткових обмежень
$\tau_1 < RS \le \tau_2$	A_2	Доступ з обмеженнями	Обмежений доступ до ресурсів
$\tau_2 < RS \le \tau_3$	A_3	Додаткова автентифікація	Посилена перевірка контексту
$RS > \tau_3$	A_4	Відмова у доступі	Блокування доступу

Інтерпретація табличної моделі

Як видно з табл. 3, інтегральний показник ризику RS відображається у формальні рішення щодо доступу шляхом порогового розбиття простору значень ризику. Таке подання забезпечує уніфіковану інтерпретацію результатів оцінювання та може бути безпосередньо використане при реалізації політик доступу або під час експериментальної валідації методу.

Поєднання формального відображення Φ_i табличної інтерпретації забезпечує математичну строгість і практичну придатність запропонованої моделі ухвалення рішень у системах контекстного контролю доступу.

Таким чином, розроблено адаптивну модель контекстного контролю доступу для підвищення стійкості КІС, яка за рахунок інтегрованого урахування технічного стану кінцевого пристрою, рівня привілеїв користувача та динамічних параметрів середовища доступу забезпечує кількісне оцінювання ризику кожного запиту доступу в режимі реального часу.

Запропонована модель реалізує ризик-орієнтований підхід до ухвалення рішень про доступ, що відповідає принципам архітектури Zero Trust, та дає можливість адаптивно змінювати політики доступу залежно від поточного контексту взаємодії,

знижуючи ймовірність несанкціонованого доступу та підвищуючи загальну кіберстійкість КІС.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті запропоновано модель адаптивного контекстного контролю доступу для КІС, побудовану на інтеграції трьох ключових груп атрибутів: технічного стану пристрою, ролі користувача та параметрів середовища доступу. На основі аналізу сучасних підходів до Zero Trust авторизації та існуючих моделей trust-score обґрунтовано необхідність поєднання цих факторів у єдину структуру оцінювання ризику. Запропонована модель дозволяє здійснювати динамічне прийняття рішень, забезпечуючи чутливість до слабких компонентів безпеки та високу точність у виявленні ризикових ситуацій.

Представлений підхід має наукову новизну завдяки формалізації вагових коефіцієнтів Device Posture, використанню множника ролі користувача та контекстно залежного коефіцієнта середовища. Мультиплікативна інтеграція цих параметрів відображає їх взаємний підсилювальний ефект, що є важливим з погляду моделювання реальних загроз, зокрема ескалації привілеїв та атак у публічних або ненадійних мережах. Запропонована функція інтегрального ризику забезпечує відповідність принципам Zero Trust, які передбачають постійне оцінювання запитів та відсутність апріорної довіри до будь-якого суб’єкта.

Практична цінність моделі полягає у можливості її застосування в системах адаптивної авторизації, де необхідно враховувати різнотипні параметри доступу в режимі реального часу. Вона може бути використана як основа для побудови механізмів автоматизованого контролю доступу, інструментів моніторингу ризиків або компонентів системи управління ідентичністю. Запропонована модель може бути особливо корисною в умовах підвищених вимог до захисту КІС, коли традиційні статичні правила доступу виявляються недостатніми.

Перспективи подальших досліджень полягають у розширенні моделі за рахунок поведінкових атрибутів, інтеграції статистичних даних та використання методів машинного навчання для адаптивного коригування коефіцієнтів та порогових значень. Окремого дослідження потребує перевірка моделі на реальних даних, зокрема визначення оптимальних порогів RS для різних типів КІС. Також перспективним є застосування моделі у комбінованих архітектурах, які інтегрують Zero Trust із концепціями кіберстійкості й автоматизованої реакції на інциденти.

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. Sandhu, R., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *IEEE Computer*, *29*(2), 38–47.
4. Hu, V. C., Ferraiolo, D. F., Kuhn, D. R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). *Guide to attribute based access control (ABAC) definitions and considerations* (NIST Special Publication 800-162). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-162
5. Jeong, S., & Yang, H. (2025). A trust score-based access control model for Zero Trust architecture. *Applied Sciences, 15*(17), 9551. https://doi.org/10.3390/app15179551

6. 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 International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1422–1429. https://doi.org/10.1109/TrustCom60117.2023.00194
7. 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
8. Lukaseder, T., Halter, M., & Kargl, F. (2020). Context-based access control and trust scores in Zero Trust campus networks. In *Sicherheit 2020: Lecture Notes in Informatics (LNI)* (pp. 53–66). Gesellschaft für Informatik. https://doi.org/10.18420/sicherheit2020_04
9. Cybersecurity and Infrastructure Security Agency. (2023). *Zero Trust maturity model (Version 2.0)*. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
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. Singh, V. (2025). Context-aware access control in SaaS environments: A metric-driven framework. *Journal of Information Systems Engineering & Management, 10*(58s), Article 12768. https://doi.org/10.52783/jisem.v10i58s.12768
12. Herrera, J. L., Chen, H.-Y., Berrocal, J., Murillo, J. M., & Julien, C. (2022). Context-aware privacy-preserving access control for mobile computing. *Pervasive and Mobile Computing*. https://doi.org/10.1016/j.pmcj.2022.101725
13. Автушенко, В., Козлов, Д., & Черненко, А. (2022). Аналіз методів моделювання систем захисту інформації. *Кібербезпека: освіта, наука, техніка*, *7*(2), 33–44. https://csecurity.kubg.edu.ua/index.php/journal/article/view/373

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Viktoriia Sydorenko
PhD, Associate Professor,
Associate Professor of IT-Security Academic Department
State University «Kyiv Aviation Institute», Kyiv, Ukraine
ORCID: 0000-0002-5910-0837
v.sydorenko@ukr.net

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

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

Abstract. This paper proposes an adaptive access control model for critical information systems that integrates three groups of attributes: device posture, user role, and access environment parameters. Based on the analysis of contemporary Zero Trust approaches, the necessity of multifactor risk assessment for each access request is substantiated. The developed model forms an integral risk score using weighted coefficients and contextual parameters, enabling dynamic decision-making in the form of access permission, restricted access, additional authentication, or access denial. The proposed approach improves the accuracy of identifying risky access scenarios and contributes to strengthening the resilience of critical information systems. Future research directions include extending the model with behavioral attributes, utilizing statistical incident data, applying machine learning methods for adaptive adjustment of weighting coefficients and threshold values, as well as conducting experimental validation of the proposed model.

Keywords: critical information systems, risk assessment, Zero Trust, access control, context-aware access control, adaptive access policies, device posture, resilience, cybersecurity.

REFERENCES

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 Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
3. Sandhu, R., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *IEEE Computer*, *29*(2), 38–47.
4. Hu, V. C., Ferraiolo, D. F., Kuhn, D. R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). *Guide to attribute based access control (ABAC) definitions and considerations* (NIST Special Publication 800-162). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-162
5. Jeong, S., & Yang, H. (2025). A trust score-based access control model for Zero Trust architecture. *Applied Sciences*, *15*(17), 9551. https://doi.org/10.3390/app15179551
6. 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 International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1422–1429. https://doi.org/10.1109/TrustCom60117.2023.00194
7. 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
8. Lukaseder, T., Halter, M., & Kargl, F. (2020). Context-based access control and trust scores in Zero Trust campus networks. In *Sicherheit 2020: Lecture Notes in Informatics (LNI)* (pp. 53–66). Gesellschaft für Informatik. https://doi.org/10.18420/sicherheit2020_04

9. Cybersecurity and Infrastructure Security Agency. (2023). *Zero Trust maturity model (Version 2.0)*. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
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. Singh, V. (2025). Context-aware access control in SaaS environments: A metric-driven framework. *Journal of Information Systems Engineering & Management*, *10*(58s), Article 12768. https://doi.org/10.52783/jisem.v10i58s.12768
12. Herrera, J. L., Chen, H.-Y., Berrocal, J., Murillo, J. M., & Julien, C. (2022). Context-aware privacy-preserving access control for mobile computing. *Pervasive and Mobile Computing*. https://doi.org/10.1016/j.pmcj.2022.101725
13. Avtushenko, V., Kozlov, D., & Chernenko, A. (2022). Analysis of information security system modeling methods. *Cybersecurity: Education, Science, Technique*, 7(2), 33–44. https://csecurity.kubg.edu.ua/index.php/journal/article/view/373