ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ



«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ»

Тези доповідей

29 жовтня
2026

м. Київ

Редакційна колегія:

Гайдур Г.І. – д.т.н., професор, завідувач кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Зибін С.В. – д.т.н., професор, професор кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Казмірчук С.В. - д.т.н., професор, професор кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Гахов С.О. – к.військ.н., доцент, доцент кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Марченко В.В. – д.ф., доцент кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Рекомендовано до друку кафедрою Сиситем та технологій Державного університету інформаційно-комунікаційних технологійй (протокол № 4 від 02.11.2026 р.)

Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 29 жовтня 2026 року). Навчально-науковий інститут кібербезпеки та захисту інформації, Державний університет інформаційно-комунікаційних технологій. Київ, 2026. 388 с.

Збірник призначений для науковців, викладачів, докторантів, аспірантів і студентів закладів вищої освіти, фахівців з кібербезпеки та захисту інформації, працівників органів державної влади та місцевого самоврядування. Редакційна колегія не несе відповідальності за зміст матеріалів, що опубліковані у збірнику. Тези подані в авторській редакції та відображають персональну позицію учасників конференції.

Мохонько Діана
ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ. НОРМАТИВНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ 113
Стебловський Г.В., Земляков С.О.
ВАЖЛИВІСТЬ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ НА ОСНОВІ ESET INSPECT & PROTECT 116
Гуленов І.В.
ПІДВИЩЕННЯ БЕЗПЕКИ VPN ЗА ДОПОМОГОЮ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ 120
Завгородня Євгенія Ярославівна
КІБЕРСТІЙКІСТЬ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ: УРОКИ АТАКИ INDUSTROYER2 ТА ПІДХІД НА ОСНОВІ NIST CSF 2.0 .. 123
Шимчук Г. В., Яцків П.О.,
КОНТЕКСТНА МОДЕЛЬ КЕРУВАННЯ ДОСТУПОМ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРЕДОВИЩ 126
Шимчук Г. В., Яцків П.О.
АДАПТИВНИЙ ЗАХИСТ ІОТ-МЕРЕЖ НА ОСНОВІ ОЦІНКИ ДОВІРИ ПРИСТРОЇВ ТА ДИНАМІЧНОЇ МІКРОСЕГМЕНТАЦІЇ 129
Онопрієнко М.Ю
МЕТОДИ І ТЕХНОЛОГІЇ КІБЕРАТАК, ОРГАНІЗОВАНИХ ЗА ПІДТРИМКИ НАЦІОНАЛЬНИХ ДЕРЖАВ ТА ЗАСОБИ ПРОТИДІЇ ЇМ 132
Ланде Дмитро Володимирович, Кузьмінський Віктор Сергійович
ВИЛУЧЕННЯ ТРИПЛЕТІВ ПРО КІБЕРЗАГРОЗИ З ТЕКСТОВИХ ПОВІДОМЛЕНЬ ІЗ ГАРАНТОВАНОЮ МЕЖЕЮ ЧАСТКИ ПОМИЛОК 135
Четвертуха Н.Р., Отенко В.І.
ВИБІР ІНСТРУМЕНТУ ДИНАМІЧНОГО АНАЛІЗУ ДЛЯ ШКІДЛИВИХ ПРОГРАМ, ЯКІ ПРИХОВУЮТЬ СВОЮ ПОВЕДІНКУ 138
Опірський І.Р., Стефанків А.В.
МЕХАНІЗМИ ВІДБОРУ ОЗНАК СИГНАЛІВ У СИСТЕМАХ РАДІОЧАСТОТНОГО ФІНГЕРПРИНТИНГУ НА ОСНОВІ НЕЙРОННИХ МЕРЕЖ 141
Афонін М.В.
АКТУАЛЬНІ ПРОБЛЕМИ БЕЗПЕКИ ІНСТРУМЕНТІВ ВІДДАЛЕНОГО ДОСТУПУ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ 144
Гончаренко М.
ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ МЕРЕЖЕВИХ АТАК У ПРОМИСЛОВИХ МЕРЕЖАХ MODBUS TCP НА ОСНОВІ АЛГОРИТМУ XGBOOST 147
Ступченко А.О
ПОБУДОВА ЦЕНТРУ ОПЕРАЦІЙНОЇ БЕЗПЕКИ (SOC) ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ОРГАНІЗАЦІЇ 150

Шимчук Г. В.,
старший викладач каф. КН,
ТНТУ ім. І. Пулюя,
Тернопіль, Україна
Яцків П.О.,
студент групи КТ-12,
ТНТУ ім. І. Пулюя,
Тернопіль, Україна

КОНТЕКСТНА МОДЕЛЬ КЕРУВАННЯ ДОСТУПОМ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРЕДОВИЩ

Запропоновано контекстну модель керування доступом до хмарних ресурсів, що поєднує принципи Zero Trust, оцінювання ризику ідентичності, стану пристрою або робочого навантаження, поведінкових відхилень, мережевого контексту та чутливості ресурсу. Модель передбачає чотири реакції: дозвіл, посилену автентифікацію, обмежений доступ і відмову. На модельному наборі зі 120 запитів 59 із 60 ризикових сценаріїв активували додаткові засоби контролю, тоді як серед нормальних запитів лише два потребували повторної перевірки.

Ключові слова: Cloud Security Alliance, Zero Trust, API, IAM, MFA

Поширення хмарних і мультихмарних архітектур істотно змінює модель захисту інформаційних систем. Традиційне припущення, що ресурс усередині корпоративного периметра є більш довіреним, поступово втрачає практичну цінність: користувачі працюють віддалено, сервіси взаємодіють між різними хмарами, а значна частина доступу виконується не людьми, а сервісними обліковими записами та програмними навантаженнями. У звіті Cloud Security Alliance серед найкритичніших хмарних ризиків визначено помилки конфігурації, недоліки керування ідентичностями та доступом, небезпечні API, недостатню видимість середовища і неконтрольований спільний доступ [1]. Тому захист хмарної системи доцільно будувати не лише на статичних ролях, а на безперервному аналізі контексту кожного запиту.

Архітектура Zero Trust формалізує підхід, за якого мережеве розташування саме по собі не є підставою для довіри. NIST SP 800-207 вимагає виконувати автентифікацію й авторизацію до встановлення сесії та розглядати ресурс, користувача і пристрій як окремі об’єкти політики [2]. Для cloud-native і multi-cloud середовищ NIST SP 800-207A додатково акцентує ідентичність застосунків і сервісів, використання API-шлюзів, service mesh і точок примусового застосування політик [3]. Практична проблема полягає в тому, що класична рольова модель RBAC здебільшого відповідає на питання «чи має суб’єкт право?», але недостатньо враховує «за яких умов це право використовується саме зараз».

Метою роботи є розроблення компактної контекстної моделі прийняття рішення про доступ, придатної для інтеграції з IAM, API Gateway, service mesh або хмарним policy engine. Для кожного запиту пропонується формувати п’ять нормованих показників у діапазоні від 0 до 1. Перший характеризує ризик ідентичності: наявність MFA, тип облікового запису, надмірність ролі, вік і

спосіб отримання облікових даних. Другий відображає ризик пристрою або робочого навантаження: стан оновлень, відповідність політикам, наявність підтвердженої workload identity та цілісність середовища виконання. Третій описує поведінкове відхилення: нетиповий час входу, різку зміну частоти запитів, звернення до незвичних ресурсів. Четвертий враховує мережевий контекст: репутацію адреси, географічну аномалію, використання анонімізаторів, відкритість точки входу. П’ятий показник задає чутливість ресурсу.

Інтегральний ризик визначається як зважена сума чотирьох динамічних складових: 30 % припадає на ризик ідентичності, 25 % – на стан пристрою або workload, 25 % – на поведінкове відхилення, 20 % – на мережевий контекст. Отримане значення додатково масштабується коефіцієнтом чутливості ресурсу, щоб однаковий контекст приводив до жорсткішого рішення для секретів, адміністративних API чи баз даних. Запропоновано чотири інтервали реакції. За низького ризику запит дозволяється відповідно до принципу найменших привілеїв, за помірного виконується step-up перевірка, наприклад повторна MFA, за підвищеного видається короткоживучий токен з обмеженням операцій до читання або окремого API, за високого ризику доступ блокується, а подія передається до SIEM/SOC.

Запропонована схема не скасовує RBAC або ABAC, а доповнює їх контекстним рівнем. Спочатку policy engine перевіряє базове право суб’єкта на ресурс. Лише після цього виконується оцінювання поточного ризику і, за необхідності, звужується вже надане право. Такий порядок зменшує небезпеку «розростання привілеїв» і компрометації легітимних облікових записів. Окремо передбачено використання короткоживучих ідентифікаційних даних для сервісів, регулярну ротацію секретів, журналювання всіх рішень policy engine та кореляцію з CloudTrail/Azure Activity Log або аналогічними джерелами. Це забезпечує можливість ретроспективної перевірки, чому конкретний запит було дозволено, обмежено чи відхилено.

Для первинної перевірки поведінки моделі проведено відтворюваний модельний експеримент із фіксованим генератором випадкових чисел. Сформовано 120 запитів чотирьох типів: 60 нормальних, 20 з аномальним контекстом, 20 із ознаками компрометації ідентичності та 20 від недовіреного робочого навантаження. Для кожного запиту генерувалися п’ять нормованих параметрів відповідно до типового профілю сценарію. Модельний набір не є заміною журналів реальної хмарної платформи, його завданням було перевірити логіку порогових рішень та оцінити співвідношення між чутливістю контролю і кількістю зайвих перевірок.

Середнє значення інтегрального ризику для нормальних запитів становило 0,133, для аномального контексту – 0,407, для компрометованої ідентичності – 0,546, для недовіреного workload – 0,521. Із 60 нормальних запитів 58 були дозволені без додаткових дій, а два спрямовані на посилену автентифікацію, жоден нормальний запит не був обмежений або заблокований. Серед 60 ризикових сценаріїв лише один запит потрапив до інтервалу безумовного

дозволу. Для 17 запитів застосовано step-up автентифікацію, для 40 – обмежений режим, для двох – повну відмову. Отже, 98,3 % модельних ризикових запитів активували додатковий контроль, а частка зайвих перевірок серед нормальних становила 3,3 %.

Наведені результати слід інтерпретувати як перевірку алгоритмічної логіки, а не як оцінку промислового продукту. У реальній інфраструктурі ваги та пороги мають адаптуватися до типу сервісу, профілю користувача і вартості помилкового блокування. Сучасні дослідження динамічного Zero Trust доступу підтверджують доцільність поєднання атрибутів, оцінки довіри та контекстних правил для хмарних середовищ [4].

Практичне впровадження моделі може виконуватися поетапно. На першому етапі збираються журнали IAM, API-шлюзів, мережевих засобів і засобів керування кінцевими пристроями без автоматичного блокування. На другому етапі policy engine працює у режимі рекомендацій, що дає змогу відкоригувати ваги та пороги. Після стабілізації профілів активуються step-up перевірка і обмеження токенів, а повна відмова залишається для явно критичних комбінацій ознак. Такий перехід зменшує ризик масових хибних блокувань і дозволяє інтегрувати контекстний контроль у чинні процеси DevSecOps.

Окремим завданням є захист самого механізму прийняття рішень. Телеметрія, що використовується для розрахунку ризику, повинна надходити з автентифікованих джерел, мати узгоджені часові мітки та бути захищеною від підміни. Журнали рішень доцільно зберігати окремо від робочих журналів застосунків, щоб компрометація одного сервісу не дозволяла приховати зміну політики. Для критичних сервісів необхідно визначити режим роботи під час недоступності policy engine: «fail closed» для адміністративних операцій і контрольований короткочасний кеш для операцій, де повне блокування створює неприйнятний ризик доступності. Важливим є також контроль версій policy-as-code, обов’язковий review змін і автоматичне тестування політик перед розгортанням.

Таким чином, для хмарних середовищ доцільно доповнювати статичне призначення ролей контекстним ризик-орієнтованим рішенням для кожної сесії. Запропонована модель узгоджується з принципами Zero Trust, враховує ідентичність, стан workload, поведінкові та мережеві ознаки й чутливість ресурсу. Модельний експеримент показав можливість відокремлювати нормальні запити від ризикових без значного збільшення кількості зайвих блокувань.

Перелік посилань:

1. Cloud Security Alliance. Top Threats to Cloud Computing 2024. 2024. URL: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024.

2. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. 2020. https://doi.org/10.6028/NIST.SP.800-207.

3. Chandramouli R., Butcher Z. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments. NIST Special Publication 800-207A. 2023. https://doi.org/10.6028/NIST.SP.800-207A.

4. Wang R., Li C., Zhang K., Tu B. Zero-trust based dynamic access control for cloud computing. Cybersecurity. 2025. Vol. 8. Art. 12. https://doi.org/10.1186/s42400-024-00320-x.