УДК 004.056.5

Аллахвердієв О.Е
Грицак А.В.

АНАЛІЗ МЕТОДІВ ДИНАМІЧНОГО КОНТРОЛЮ ДОСТУПУ З УРАХУВАННЯМ РІВНЯ РИЗИКУ

Вінницький Національний Технічний Університет

Анотація

В даній статті розглянуто аналіз методів динамічного контролю доступу з урахуванням рівня ризику. Наведено їх особливості, переваги та недоліки. Здійснено порівняння проаналізованих методів..

Ключові слова: Захист, контроль доступу

Abstract

This article analyzes the methods of dynamic access control based on the level of risk. Their features, advantages and disadvantages are presented. A comparison of the analyzed methods is made.

Key words: Protection, access control

Вступ

Динамічний контроль доступу є ключовим компонентом сучасних інформаційних систем, що забезпечує адаптивне управління доступом до ресурсів залежно від умов та контексту. У зв'язку зі зростанням складності кіберзагроз і підвищенням вимог до захисту інформації, традиційні методи управління доступом втрачають свою ефективність, що зумовлює необхідність впровадження нових підходів.

Особливу увагу привертають методи динамічного контролю доступу, які враховують рівень ризику для визначення прав доступу. До таких методів належать адаптивний контроль на основі ризику, політики на основі атрибутів, використання штучного інтелекту, динамічна багатофакторна аутентифікація та поведінковий аналіз. Кожен із цих підходів має свої переваги та недоліки, що вимагає їх детального аналізу для оцінки доцільності використання в конкретних умовах.

Метою статті є аналіз і порівняння сучасних методів динамічного контролю доступу з урахуванням рівня ризику, їхньої ефективності, гнучкості та ресурсомісткості. Представлений аналіз допоможе визначити оптимальні рішення для забезпечення безпеки інформаційних систем у динамічному середовищі..

Дослідження

Адаптивний контроль доступу на основі ризику є сучасним підходом до забезпечення безпеки інформаційних систем, який динамічно змінює рівень доступу до ресурсів залежно від оцінки ризиків, пов’язаних із кожним запитом користувача. Цей метод відрізняється від традиційних систем управління доступом своєю здатністю реагувати на зміни в умовах доступу в режимі реального часу, забезпечуючи адаптивність до динамічних загроз.

У основі адаптивного контролю доступу лежить аналіз різноманітних факторів, що формують рівень ризику запиту. До таких факторів належать поведінкові характеристики користувача, параметри запиту (місцезнаходження, пристрій, IP-адреса), час доступу, тип ресурсу та історичні дані про дії користувача. Наприклад, якщо користувач намагається отримати доступ із нового пристрою або з іншого географічного розташування, система оцінює ці зміни як підвищений ризик і може знизити рівень доступу або запитати додаткову автентифікацію, наприклад, через SMS-код або біометрію.

Однією з головних переваг цього методу є його гнучкість. Адаптивний контроль доступу дозволяє знижувати ймовірність компрометації даних, зберігаючи зручність для користувачів. Легітимні дії користувачів у звичних умовах виконуються без зайвих перевірок, тоді як підозрілі дії піддаються додатковій перевірці або блокуються. Такий підхід також дозволяє мінімізувати втручання адміністратора, оскільки система самостійно приймає рішення на основі заданих політик і алгоритмів оцінки ризику [1].

Ще однією важливою перевагою є можливість інтеграції з іншими компонентами системи безпеки, такими як інструменти аналізу поведінки (UEBA) або системи виявлення вторгнень (IDS). Це дозволяє не лише контролювати доступ, а й виявляти потенційні загрози на ранніх етапах.

Однак адаптивний контроль доступу має і свої недоліки. Реалізація такого методу вимагає складного налаштування та постійного моніторингу. Необхідно правильно визначити критерії оцінки ризиків, щоб уникнути хибнопозитивних або хибнонегативних результатів.

У сучасних умовах адаптивний контроль доступу на основі ризику є одним із найбільш перспективних методів захисту, особливо для великих систем із високою динамікою запитів. Його застосування особливо актуальне у фінансових, медичних, корпоративних та державних інформаційних системах, де захист даних є критично важливим. Інтеграція такого підходу дозволяє значно підвищити рівень безпеки, забезпечуючи баланс між гнучкістю доступу та його захищеністю.

Політики на основі атрибутів і контексту є сучасним підходом до управління доступом, який забезпечує високий рівень гнучкості та безпеки шляхом врахування сукупності атрибутів і умов доступу. Цей метод відрізняється від традиційних систем управління доступом (таких як рольовий доступ) тим, що прийняття рішення про доступ ґрунтується на атрибутах користувача, ресурсу, до якого запитується доступ, а також контексту, в якому цей запит здійснюється [2].

Наприклад, співробітник може отримати доступ до корпоративних документів лише в робочий час із офісної мережі та на авторизованому пристрої. Якщо запит здійснюється з іншої мережі або поза робочим часом, система може обмежити доступ або запитати додаткову автентифікацію.

Переваги політик на основі атрибутів і контексту очевидні. По-перше, такий підхід забезпечує детальний контроль за доступом, дозволяючи враховувати численні умови, які впливають на рівень безпеки. Це значно підвищує захищеність інформаційної системи, оскільки доступ надається лише за суворої відповідності всіх атрибутів і контексту. По-друге, цей метод є надзвичайно гнучким і може бути адаптований до різноманітних умов, зокрема для специфічних вимог окремих організацій. Наприклад, у медичних системах доступ до даних пацієнта може залежати не лише від ролі користувача, але й від того, чи бере він участь у поточному лікуванні цього пацієнта [2].

Проте існують і недоліки, які слід враховувати. Основним викликом є складність налаштування та підтримки таких політик. Врахування багатьох параметрів вимагає ретельного моделювання системи доступу, а також постійного моніторингу змін у контексті чи атрибутах. Наприклад, якщо змінюються організаційні структури або додаються нові типи ресурсів, політики доступу необхідно оновлювати, щоб забезпечити їх актуальність. Ще одним недоліком є те, що система може споживати значні ресурси для обробки атрибутів і контексту, особливо в масштабних системах із великим числом запитів.

Іншою проблемою є потенційна складність діагностики та усунення помилок у налаштуваннях політик. Наприклад, якщо доступ був несподівано обмежений, може бути важко швидко визначити, який саме атрибут або умова спричинили це рішення. Це може ускладнити управління системою, особливо для великих організацій із тисячами користувачів і ресурсів [2].

Застосування цього методу є доцільним у системах, де критично важливим є врахування умов доступу. Це включає корпоративні системи з багатьма рівнями конфіденційності, системи електронного урядування, медичні та фінансові установи, а також хмарні сервіси. Наприклад, у хмарних системах доступ може залежати від географічного місця користувача або типу підписки.

Використання AI та машинного навчання у динамічному контролі доступу є одним із найбільш перспективних напрямів розвитку інформаційної безпеки. Цей підхід ґрунтується на здатності алгоритмів штучного інтелекту аналізувати великі обсяги даних і виявляти складні закономірності, що можуть бути недоступними для традиційних методів управління доступом. Застосування AI дозволяє системам не лише автоматично приймати рішення про доступ, але й адаптуватися до змін у середовищі, прогнозуючи ризики і реагуючи на потенційні загрози.

Основою цього методу є використання алгоритмів машинного навчання, які аналізують поведінку користувачів, типи запитів, історичні дані про доступ та інші атрибути.

Однією з основних переваг використання AI є здатність до постійного самонавчання. Алгоритми можуть вдосконалювати свої моделі, базуючись на нових даних, що надходять із системи. Це дозволяє системам бути ефективними навіть у випадках, коли загрози є новими і раніше не були зареєстровані. Наприклад, система може виявити нові патерни аномальної активності, що свідчать про можливу компрометацію доступу, навіть якщо вони не відповідають жодному з відомих шаблонів загроз.

Ще однією значною перевагою є швидкість обробки даних. AI здатен у реальному часі аналізувати величезні обсяги інформації, що включають дані про поведінку користувачів, контекст доступу, мережеві характеристики та інші фактори. Це дозволяє швидко приймати рішення про надання доступу або блокування запитів, що особливо важливо для великих організацій або систем із високим навантаженням [3].

Однак використання AI та машинного навчання має і свої недоліки. По-перше, впровадження таких систем вимагає значних ресурсів, включаючи високопродуктивне обладнання для обробки даних, а також великий обсяг якісних даних для навчання моделей. Без належного обсягу та якості даних результати роботи AI можуть бути ненадійними. По-друге, існує ризик помилкових спрацювань, коли

легітимні дії користувачів помилково оцінюються як потенційна загроза. Це може викликати незручності для користувачів, а також додаткове навантаження на систему підтримки.

Ще одним викликом є тлумачення рішень, прийнятих AI. Алгоритми, особливо ті, що базуються на глибокому навчанні, часто функціонують як "чорна скринька", і розуміння причин, чому конкретний запит був заблокований чи дозволений, може бути ускладненим. Це може створювати проблеми для адміністраторів і впливати на довіру до системи.

Попри ці недоліки, AI та машинне навчання відкривають нові можливості в управлінні доступом. Їхнє використання є особливо ефективним у великих і складних системах, де традиційні методи стають менш результативними через зростання обсягу даних і кількості загроз.

Динамічна багатофакторна аутентифікація (MFA) є сучасним методом забезпечення безпеки інформаційних систем, що поєднує зручність для користувачів із високим рівнем захисту від несанкціонованого доступу. Цей підхід базується на класичному принципі багатофакторної аутентифікації, який передбачає використання кількох незалежних факторів для підтвердження ідентичності користувача. Відмінною рисою динамічної MFA є її адаптивність, що дозволяє автоматично змінювати вимоги до аутентифікації залежно від рівня ризику [3].

Основна концепція динамічної MFA полягає у тому, що додаткові фактори аутентифікації запитуються тільки в ситуаціях підвищеного ризику. Наприклад, якщо користувач намагається увійти в систему з нового пристрою, незвичного місця або в нерегламентований час, система може запитати додатковий одноразовий пароль (OTP), підтвердження через мобільний додаток або біометричну автентифікацію, таку як відбиток пальця чи розпізнавання обличчя. У звичайних умовах, коли поведінка користувача відповідає встановленому шаблону, автентифікація може обмежуватися одним фактором, наприклад паролем.

Переваги динамічної MFA включають значне підвищення рівня безпеки при мінімальному дискомфорті для користувачів. Оскільки додаткові фактори запитуються лише у разі підвищеного ризику, користувачам не потрібно проходити складну процедуру автентифікації за кожного входу в систему. Це забезпечує баланс між захистом і зручністю.

Динамічна MFA також ефективно знижує ризики, пов’язані з компрометацією паролів. Навіть якщо зловмисник отримує доступ до пароля користувача, відсутність додаткових факторів автентифікації значно ускладнює йому доступ до системи. Крім того, цей метод дозволяє швидко реагувати на зміну рівня ризику в режимі реального часу, забезпечуючи високий ступінь захищеності без необхідності втручання адміністратора [3].

Недоліками динамічної MFA є певне навантаження на користувачів у разі частих запитів додаткової автентифікації, що може викликати дискомфорт. Наприклад, користувачі, які працюють у середовищах із підвищеним ризиком, можуть стикатися з необхідністю багаторазового підтвердження автентифікації протягом короткого часу. Це може негативно впливати на користувацький досвід, особливо якщо сповіщення про додаткову автентифікацію надходять із затримкою через проблеми із підключенням до мережі.

Ще одним викликом є впровадження цього методу, яке вимагає інтеграції з існуючими системами управління доступом та високоякісного програмного забезпечення для забезпечення точності й швидкості автентифікації.

Застосування динамічної MFA є доцільним у середовищах, де критично важливо забезпечити як високу безпеку, так і зручність для користувачів. Це включає корпоративні мережі, хмарні сервіси, банківські платформи та медичні інформаційні системи. Наприклад, у фінансових установах динамічна MFA може автоматично активуватися для захисту рахунків користувачів у разі спроби доступу з нових пристроїв або підозрілих місцезнаходжень [4].

Поведінковий аналіз та відстеження аномалій є одним із найбільш ефективних підходів до динамічного контролю доступу, який дозволяє ідентифікувати потенційні загрози на основі відхилень від звичайної поведінки користувача. Цей метод базується на аналізі патернів дій користувача, таких як частота доступу до ресурсів, типи виконуваних операцій, тривалість сесій і навіть стиль набору тексту або переміщення курсора.

Переваги методу полягають у його здатності виявляти навіть ті загрози, які не можуть бути ідентифіковані іншими методами контролю доступу, наприклад, інсайдерські атаки. На відміну від статичних політик доступу, поведінковий аналіз дозволяє реагувати на нові типи загроз, які раніше не були враховані. [4].

Проте існують і недоліки, які необхідно враховувати під час впровадження поведінкового аналізу. Основним викликом є необхідність збирання та зберігання великої кількості даних про дії користувачів, що може призвести до додаткових витрат на інфраструктуру. Крім того, для досягнення високої точності аналізу потрібні якісні дані, а їхня відсутність може знизити ефективність системи або призвести до помилкових спрацювань. Наприклад, якщо користувач перебуває у відрядженні і його

поведінка відрізняється від звичайної, це може бути помилково інтерпретовано як аномалія, що створить незручності для користувача.

Ще одним викликом є складність налаштування системи. Виявлення аномалій вимагає точного визначення нормальної поведінки, що може бути різним для кожного користувача або групи користувачів. Крім того, змінні умови (наприклад, сезонні зміни у поведінці або специфіка роботи в окремі дні) також мають враховуватися, щоб уникнути надмірної чутливості системи до відхилень [4].

Застосування поведінкового аналізу та відстеження аномалій є особливо актуальним у системах, де існує високий ризик інсайдерських атак або компрометації облікових записів. Наприклад, у фінансових установах цей метод дозволяє виявляти підозрілу активність, пов'язану з транзакціями, які не відповідають звичному профілю клієнта. У корпоративних системах поведінковий аналіз може ідентифікувати зловживання правами доступу, наприклад, спроби несанкціонованого доступу до конфіденційних даних.

У таблиці 1 здійснено порівняння проаналізованих методів.

Таблиця 1 − Порівняння методів динамічного контролю доступу з урахуванням рівня ризику

Метод контролю доступу	Опис	Переваги	Недоліки
Адаптивний контроль доступу на основі ризику	Динамічно оцінює ризики та коригує рівень доступу на основі поведінки користувача та параметрів запиту.	Гнучкий контроль, знижує ризики компрометації доступу, адаптивність до умов.	Складність налаштування, потребує постійного моніторингу і корекції.
Політики на основі атрибутів та контексту	Враховує атрибути користувача, ресурсів і контекст доступу (час, місце, пристрій) для визначення доступу.	Детальний контроль, можливість враховувати різні умови доступу, підвищена безпека.	Потребує розширених налаштувань та моніторингу для обліку зміни контексту.
Використання AI та машинного навчання	Аналізує великі обсяги даних для прогнозування ризиків та автоматичного коригування політик доступу.	Прогнозування загроз, постійне самонавчання, виявлення нових патернів.	Високі вимоги до ресурсів, можливість помилкових спрацювань при аномальних діях.
Динамічна багатофакторна аутентифікація (MFA)	Автоматично вимагає додаткові фактори аутентифікації при підвищеному ризику для збереження безпеки.	Баланс безпеки і зручності, адаптується до рівня ризику, посилює захист.	Додаткове навантаження на користувачів при частих запитах на MFA.
Поведінковий аналіз та відстеження аномалій	Виявляє аномалії на основі відхилення від звичайної поведінки користувача та автоматично коригує доступ.	Ефективний захист від інсайдерських загроз, автоматична реакція на аномалії.	Необхідність високоякісних даних для аналізу, ресурсоємність та налаштування SIEM/IDS.

Усі проаналізовані методи охоплюють власну сферу і забезпечують захист різними методами, тобто кожнен метод призначений під конкретну задачу

.

Висновок

У статті було проаналізовано сучасні методи динамічного контролю доступу, які базуються на різних підходах, таких як адаптивний контроль доступу на основі ризику, політики на основі атрибутів і контексту, використання штучного інтелекту та машинного навчання, динамічна багатофакторна аутентифікація і поведінковий аналіз із відстеженням аномалій. Кожен із цих методів має свої особливості, переваги та недоліки, що визначає сферу його найефективнішого застосування.

Усі проаналізовані методи спрямовані на вирішення конкретних завдань у забезпеченні безпеки інформаційних систем. Наприклад, адаптивний контроль доступу дозволяє гнучко реагувати на зміни в поведінці користувачів і умовах доступу, тоді як політики на основі атрибутів і контексту забезпечують деталізований контроль за рахунок врахування багатьох параметрів. Методи, що базуються на AI та машинному навчанні, виділяються своєю здатністю прогнозувати загрози й автоматично коригувати політики доступу, водночас поведінковий аналіз ефективно ідентифікує аномалії, пов'язані з інсайдерськими загрозами. Динамічна багатофакторна аутентифікація забезпечує баланс між зручністю для користувачів і рівнем безпеки, знижуючи ризик компрометації облікових записів.

Таким чином, кожен метод виконує специфічну роль у загальній системі захисту, а їх поєднання дозволяє створити багаторівневу систему безпеки, яка враховує різні аспекти і потреби організації. Успішне впровадження цих методів потребує аналізу конкретних вимог до системи, доступних ресурсів і рівня ризиків, що забезпечить ефективний захист інформаційних ресурсів у динамічному середовищі сучасних загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. JONES A. Adaptive Access Control and Risk Assessment [Електронний ресурс] / ALEX JONES. – 2023. – Режим доступу до ресурсу: https://www.cybersecurityinsights.org/adaptive-access-control/.
2. Behavioral Analytics in Cybersecurity: A Deep Dive [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.securityjournal.com/behavioral-analytics-cybersecurity/.
3. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://csrc.nist.gov/publications/detail/sp/800-63b/final.
4. MACHINE LEARNING TECHNIQUES. Enhancing Anomaly Detection in Access Control Systems [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.mltechjournal.com/anomaly-detection-access-control/.

Аллахвердієв Олександр Еміль огли– студент групи КІТС-23М, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: allakhverdiiev1998@gmail.com

Науковий керівник: ***Грицак Анатолій Васильович*** – кандидат технічних наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: grytsak.a.v@gmail.com

Allakhverdiev Oleksandr Emil ogly – student of KITS-23M group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail allakhverdiiev1998@gmail.com

Supervisor: ***Hrytsak Anatolii V.*** – candidate of engineering sciences, associate professor of the department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: grytsak.a.v@gmail.com